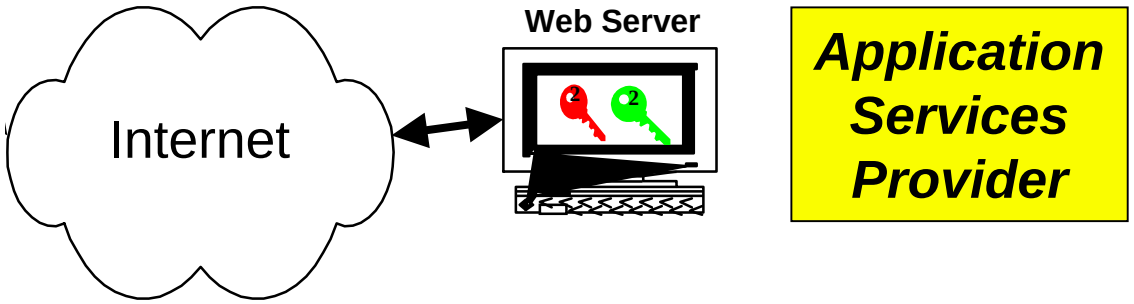
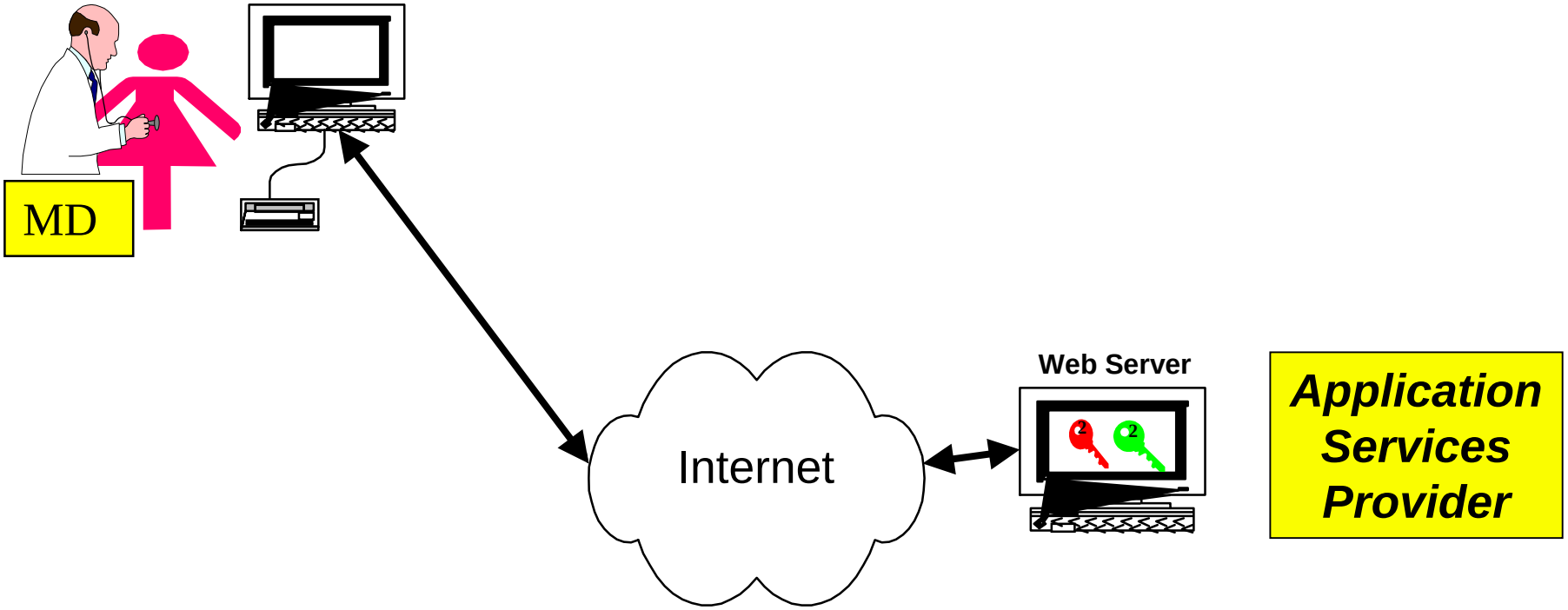
Testimony of
John T. Lynch
Vice President, ChimeTrust
to NCVHS
October 27, 2000

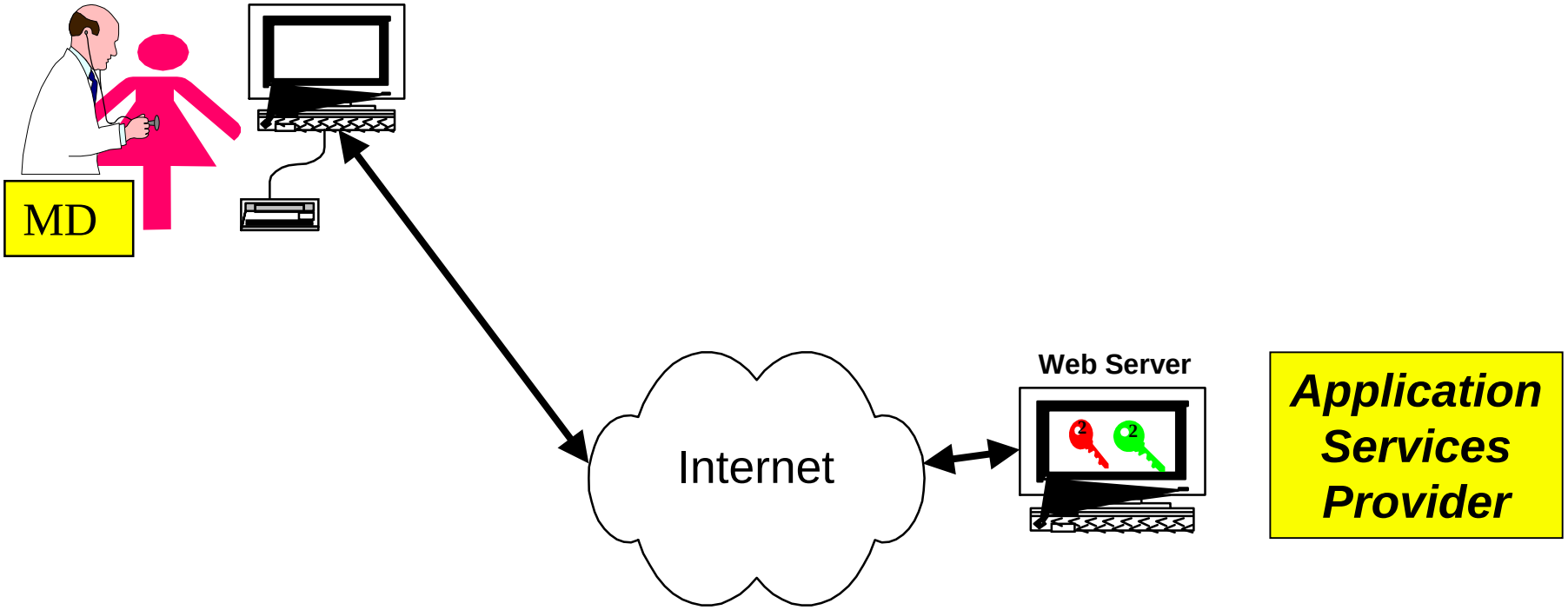
To Log On, MD Identifies Self Using Name, Pin number



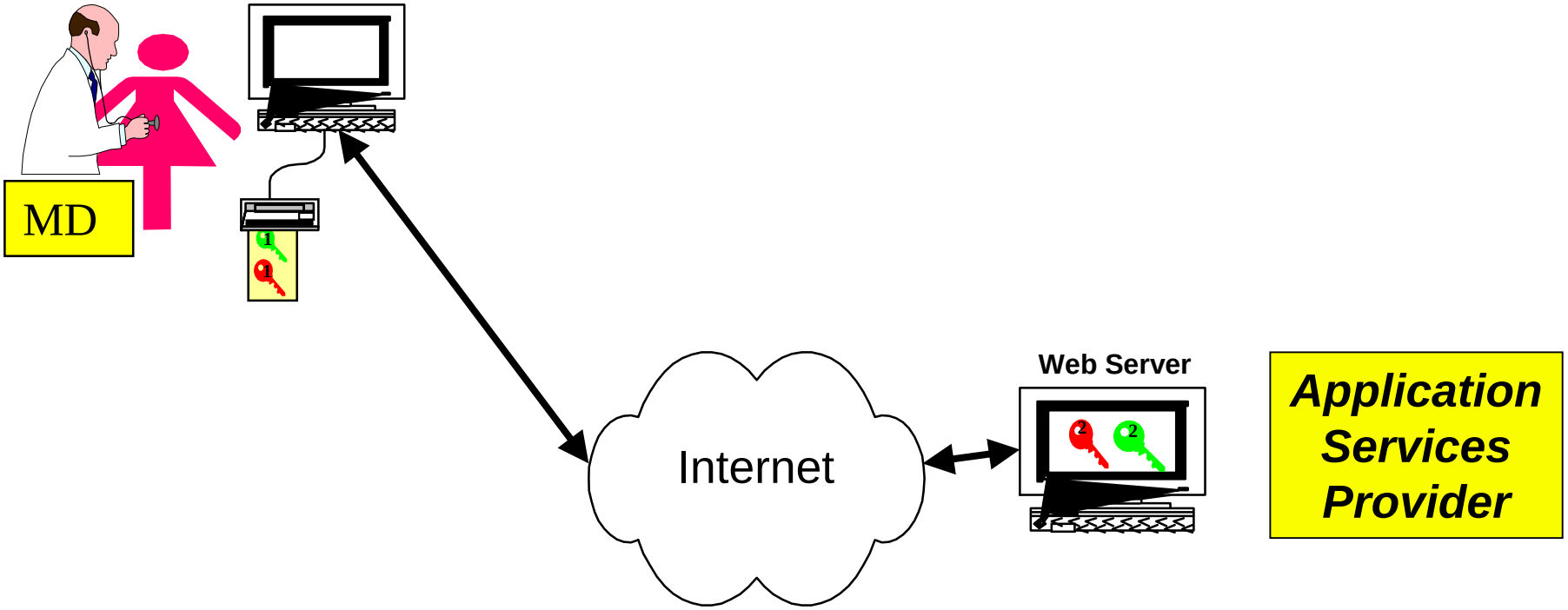
To Log On, MD Identifies Self Using Name, Pin number



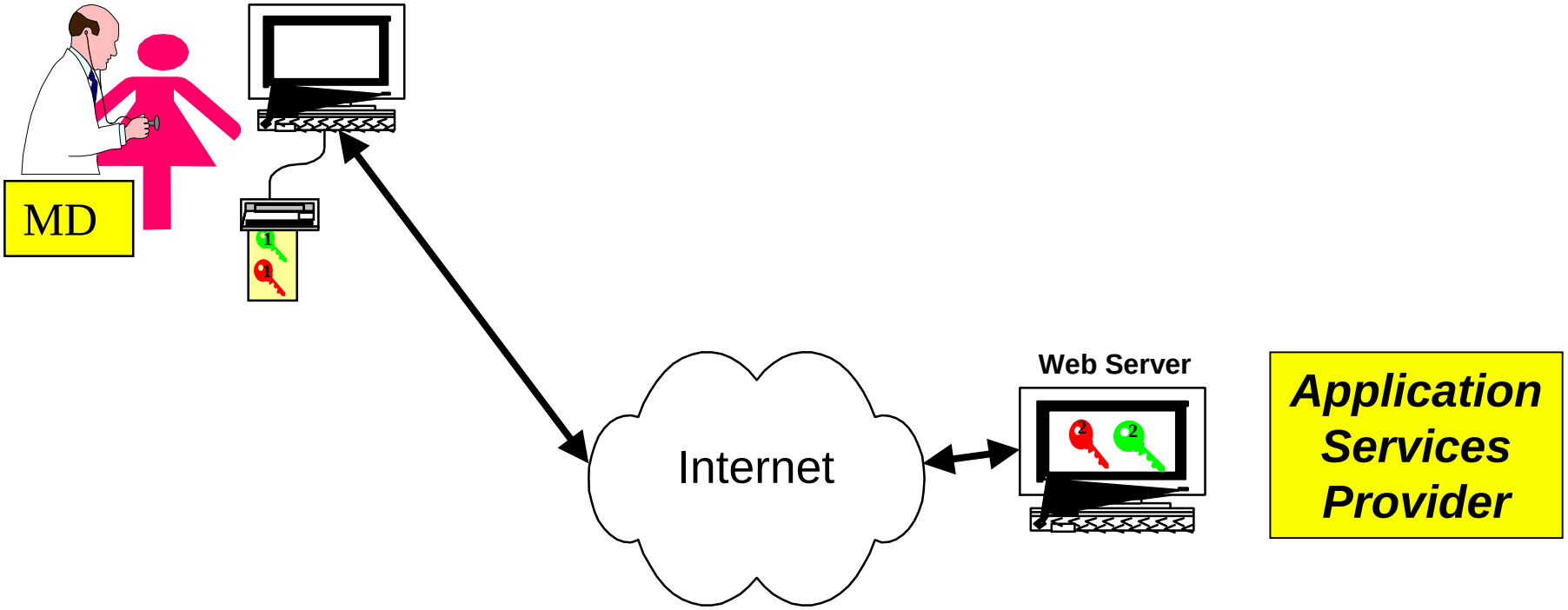
MD Authenticated using Digital Certificate on Smart Card



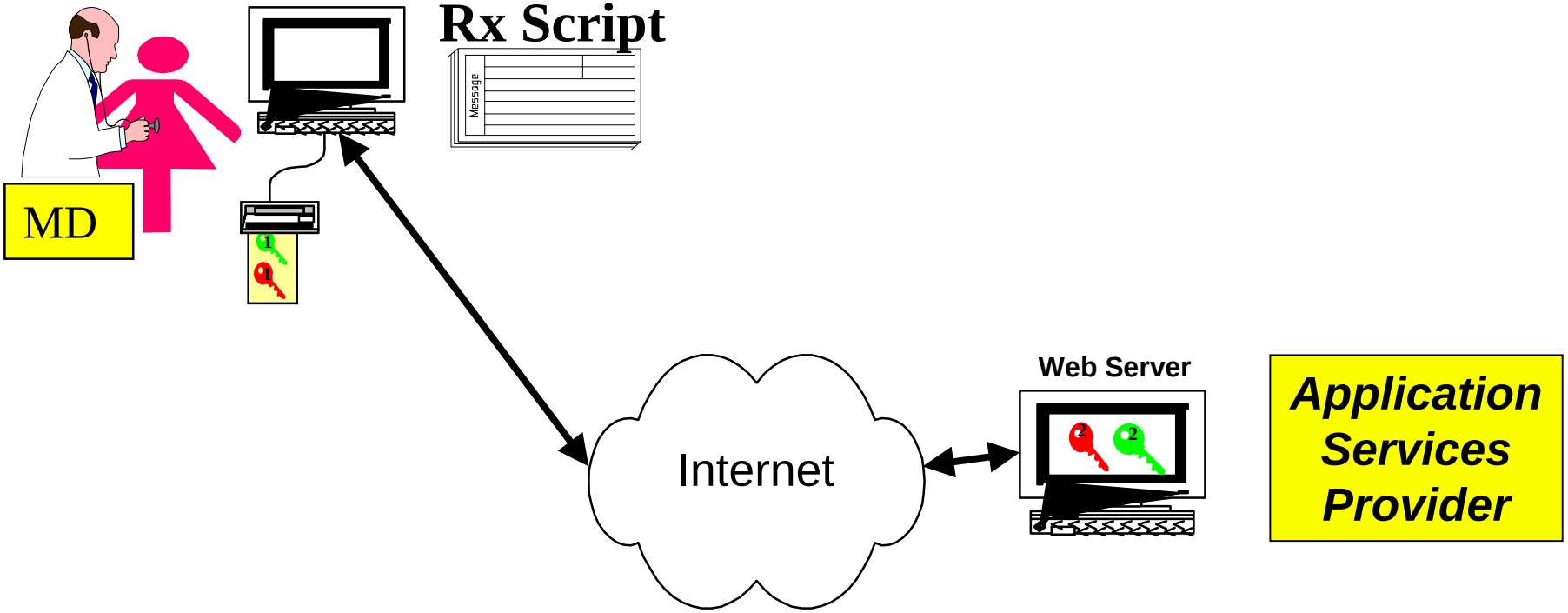
MD Authenticated using Digital Certificate on Smart Card



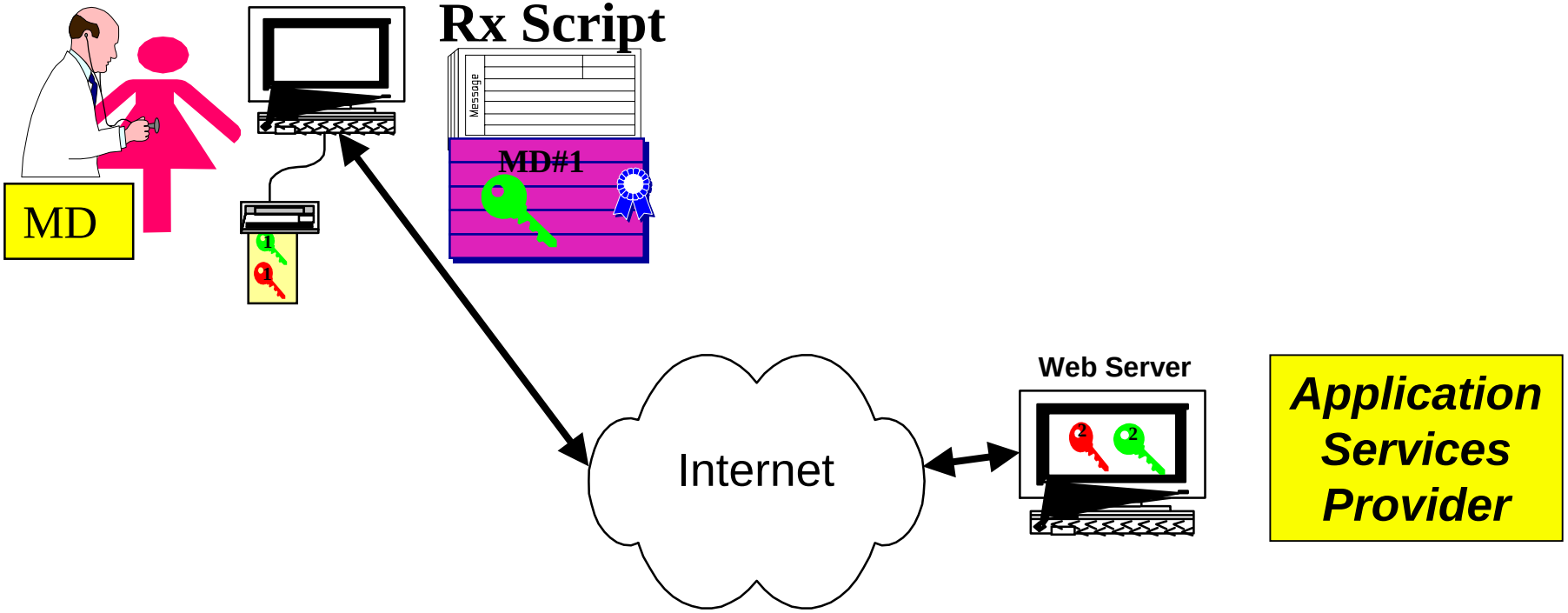
Physician writes and Signs Prescription



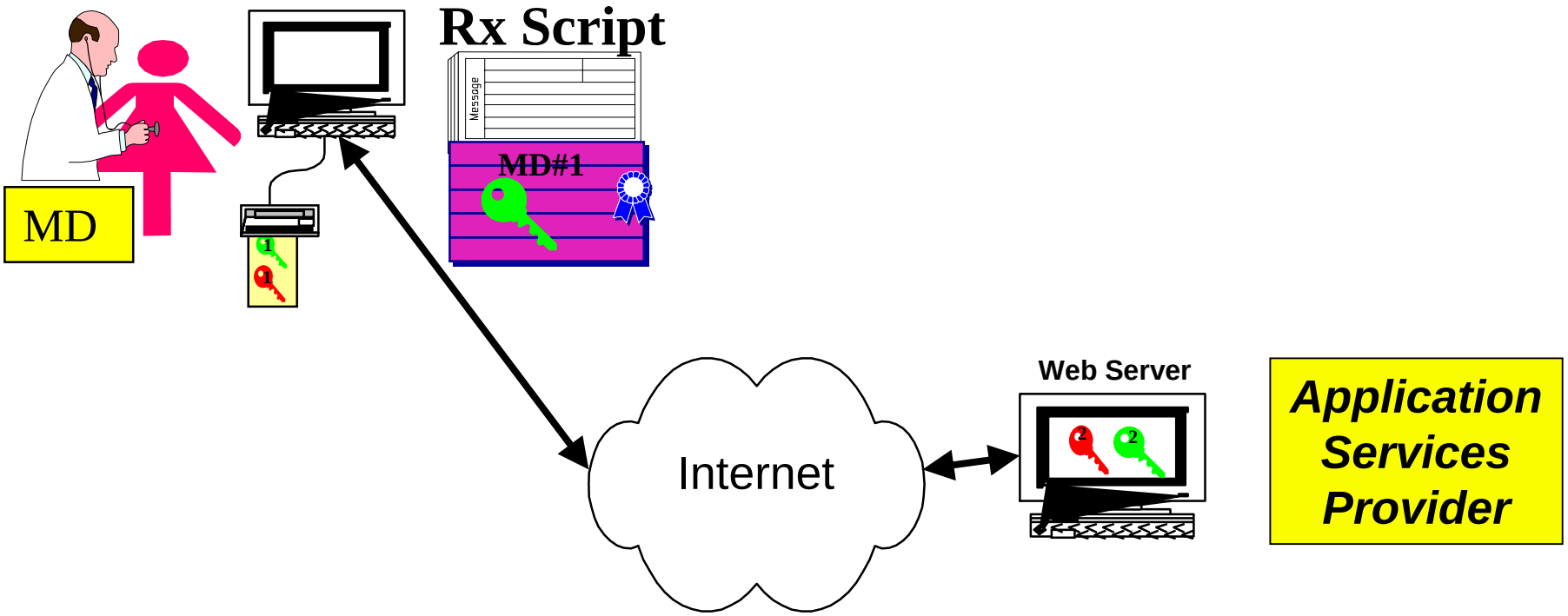
Physician writes and Signs Prescription



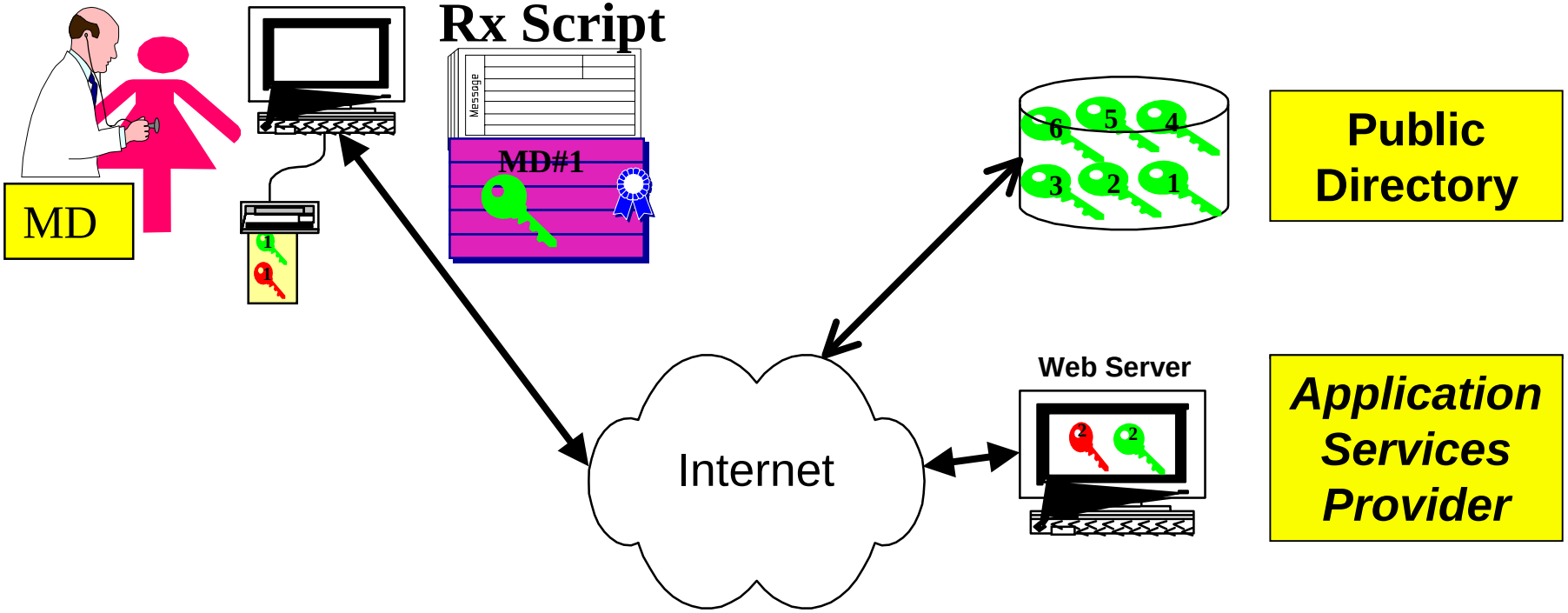
Physician writes and Signs Prescription



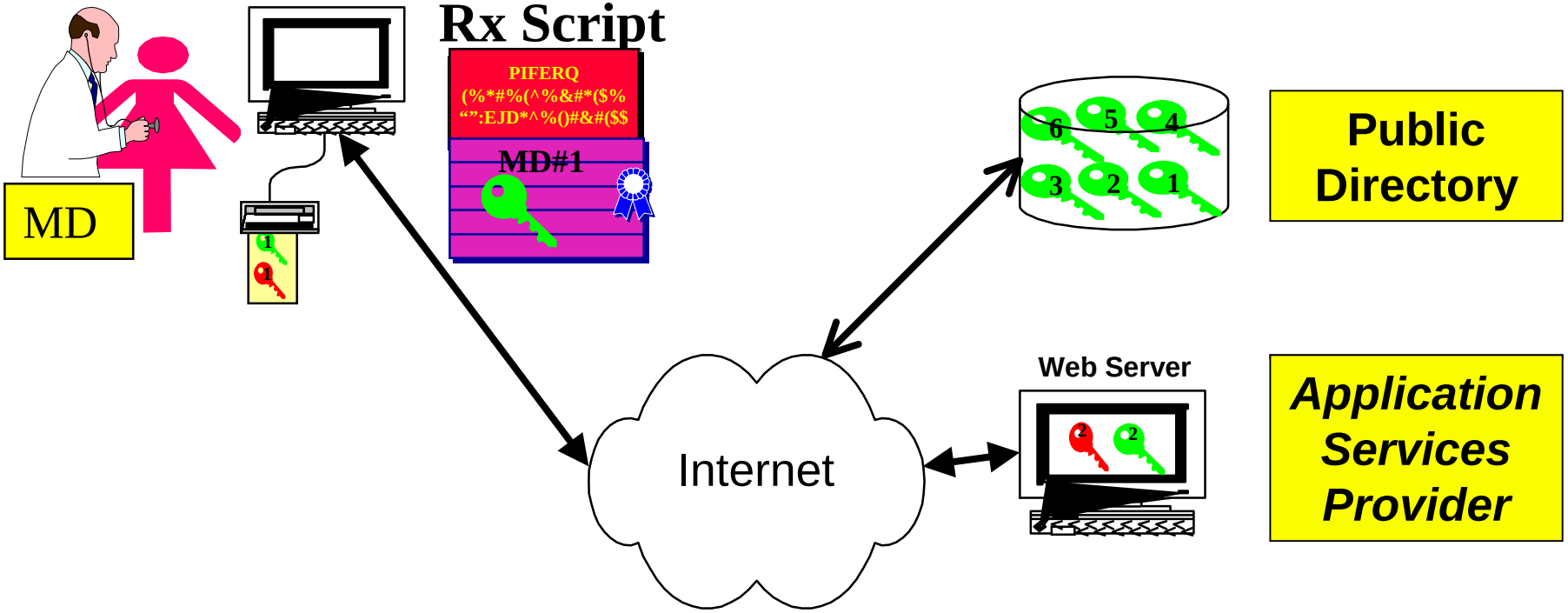
MD looks up pharmacy Public Key in Directory, encrypts script



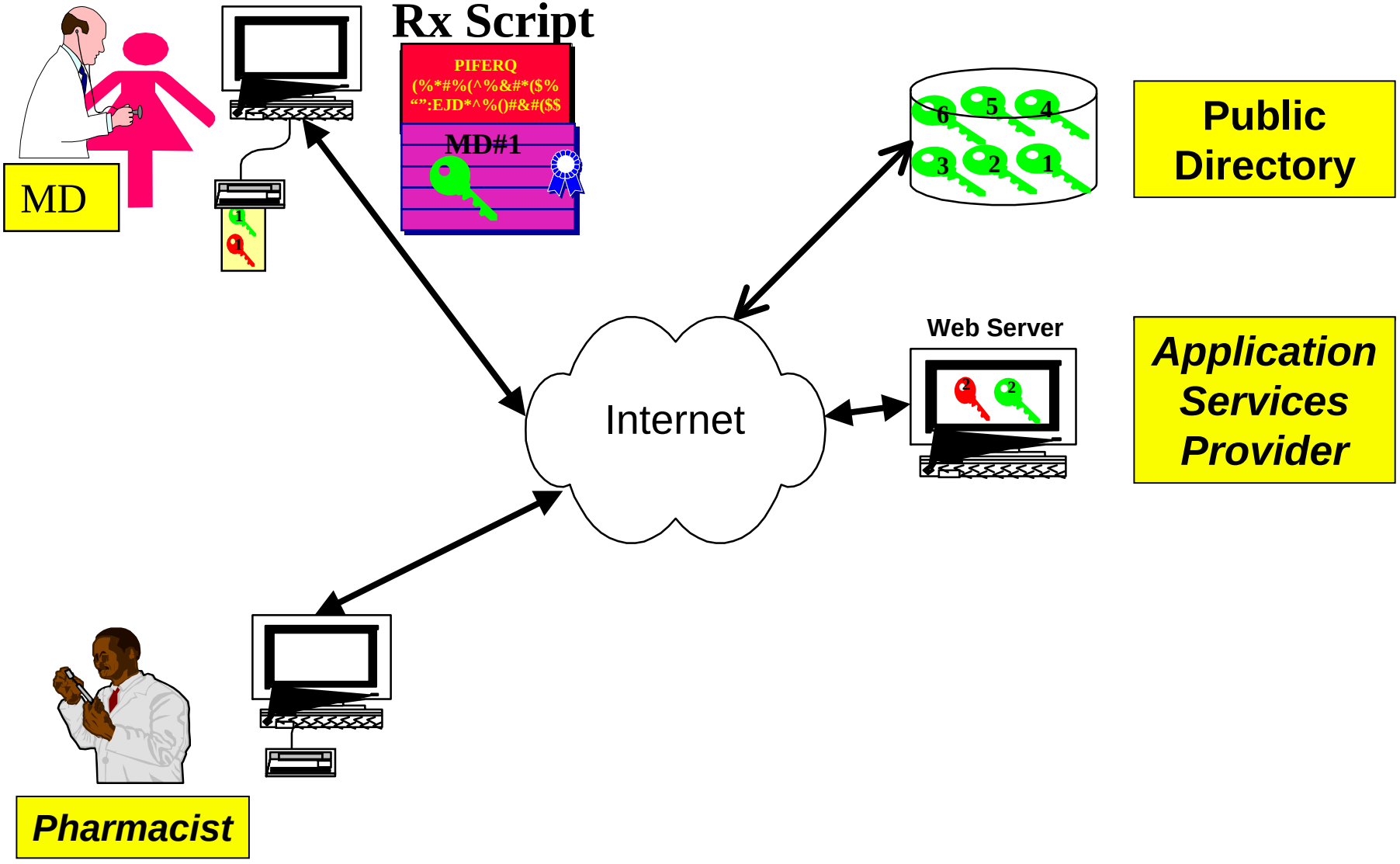
MD looks up pharmacy Public Key in Directory, encrypts script



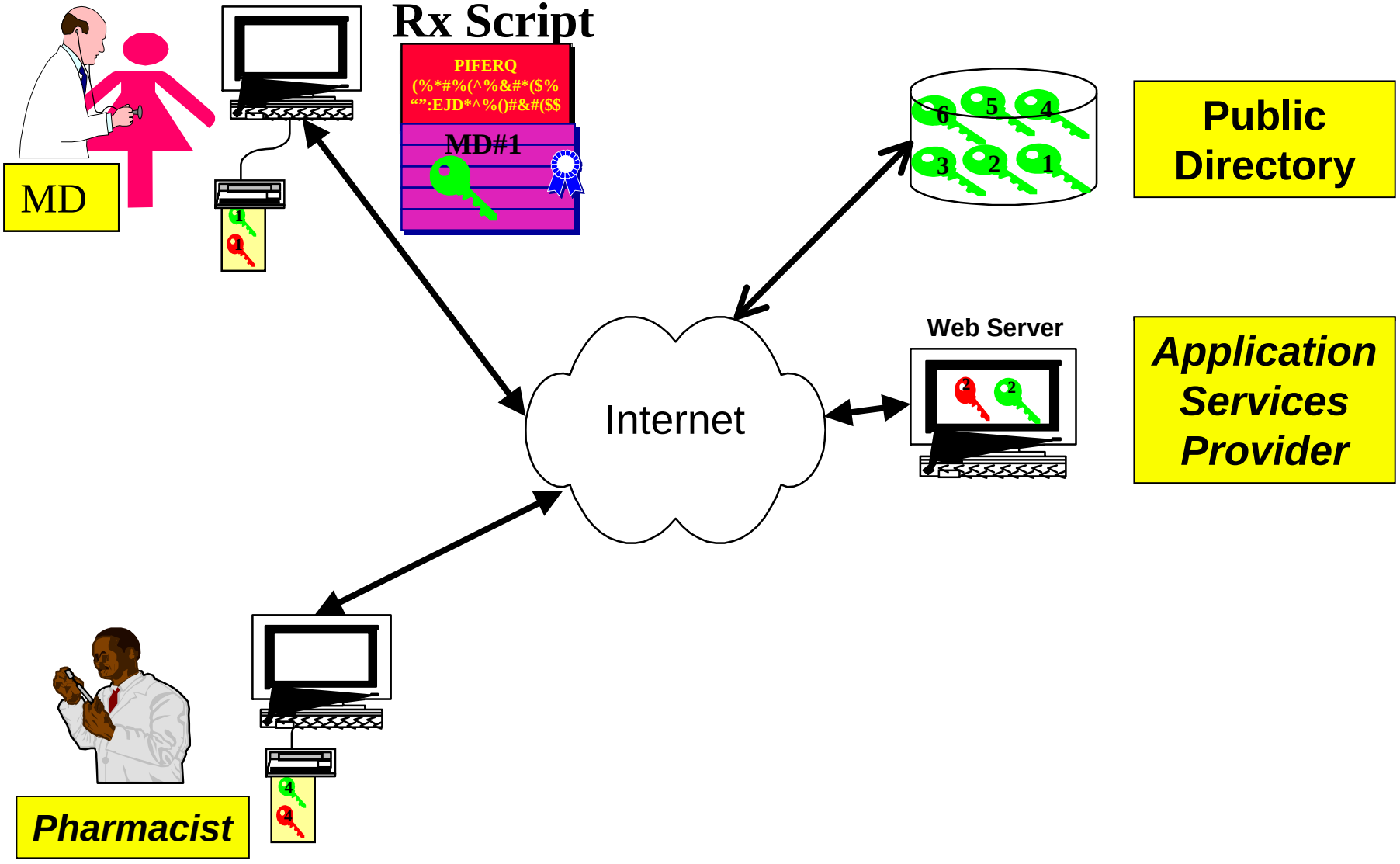
MD looks up pharmacy Public Key in Directory, encrypts script



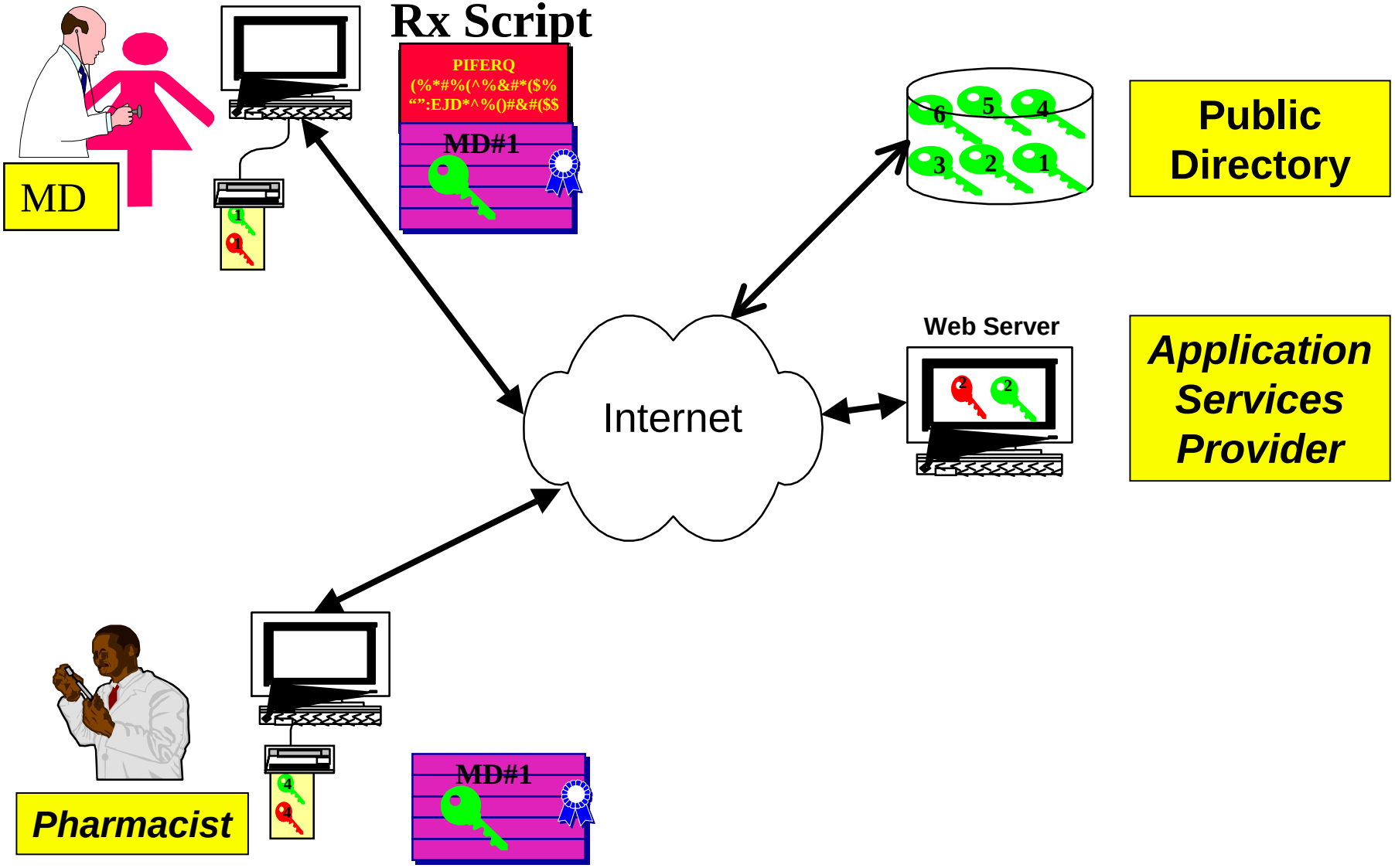
MD looks up pharmacy Public Key in Directory, encrypts script



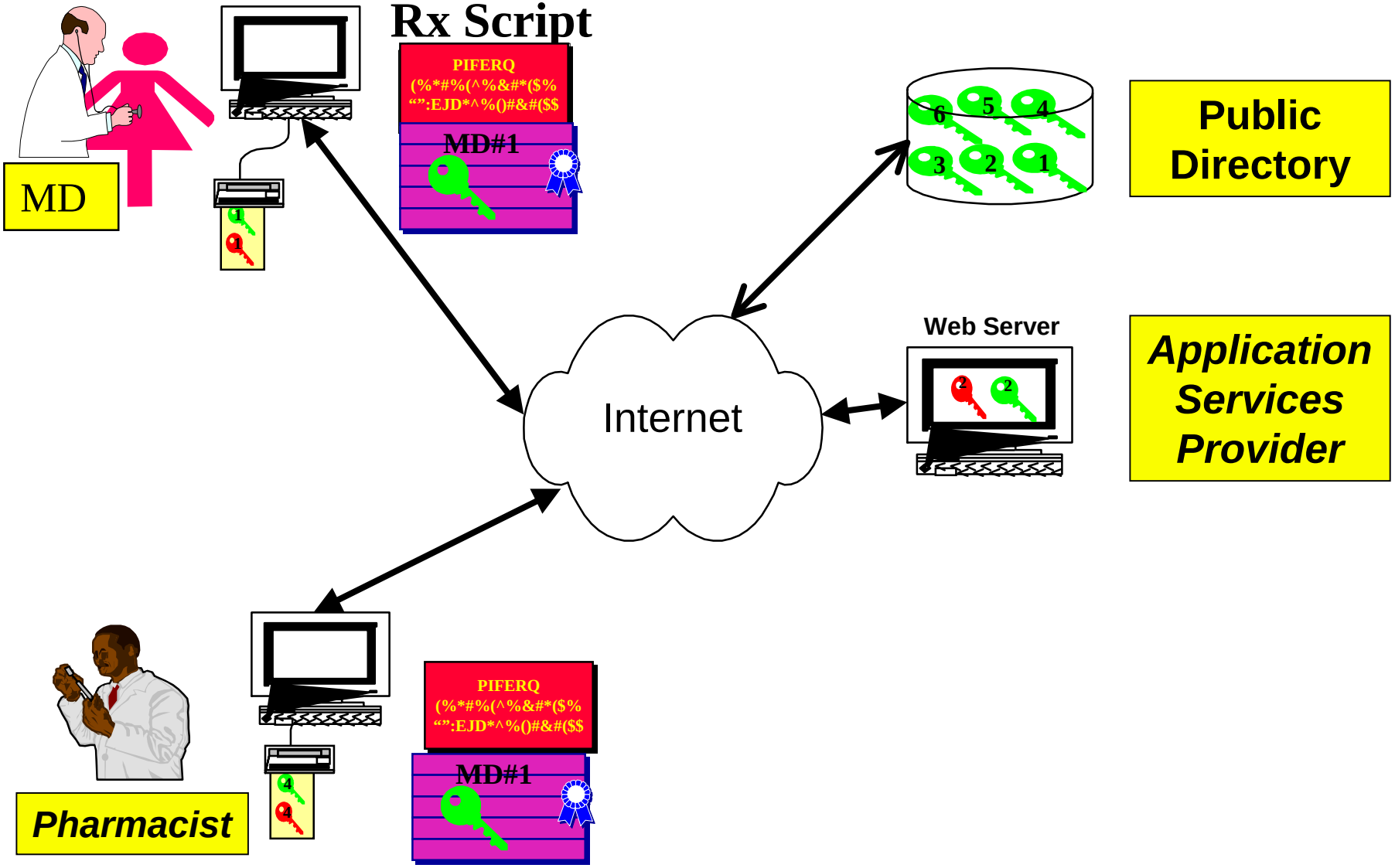
MD looks up pharmacy Public Key in Directory, encrypts script



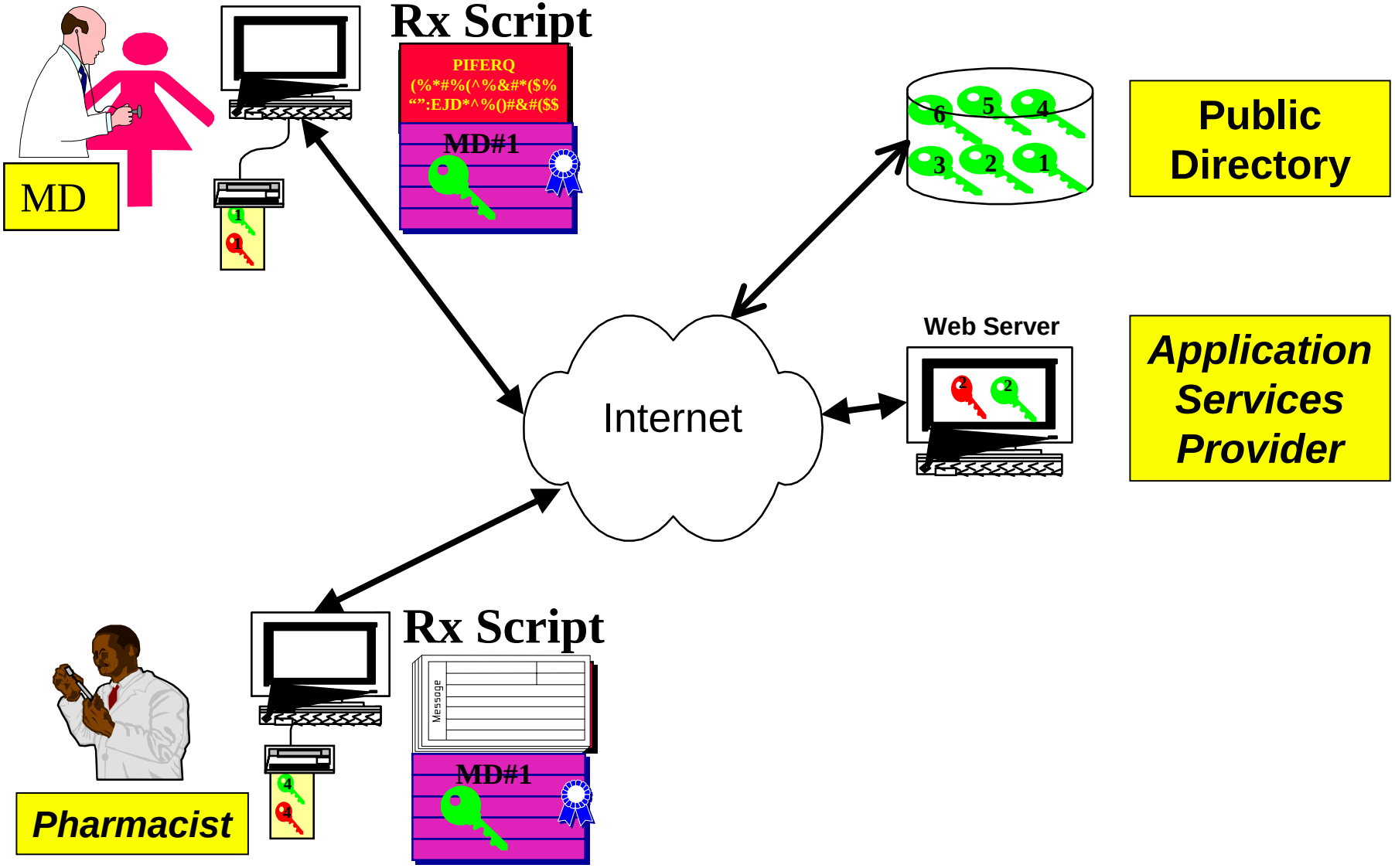
Pharmacist decrypts script



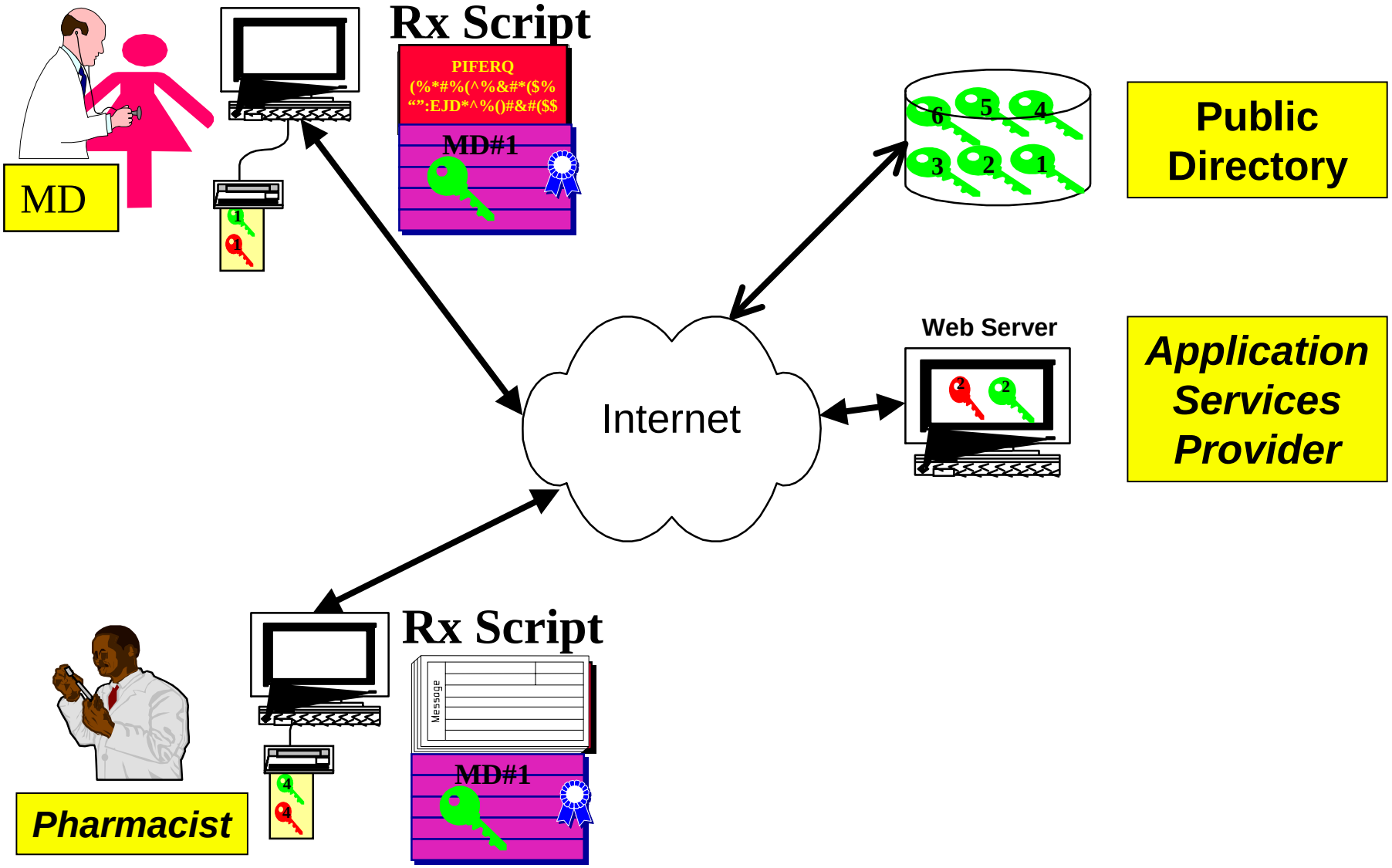
Pharmacist decrypts script



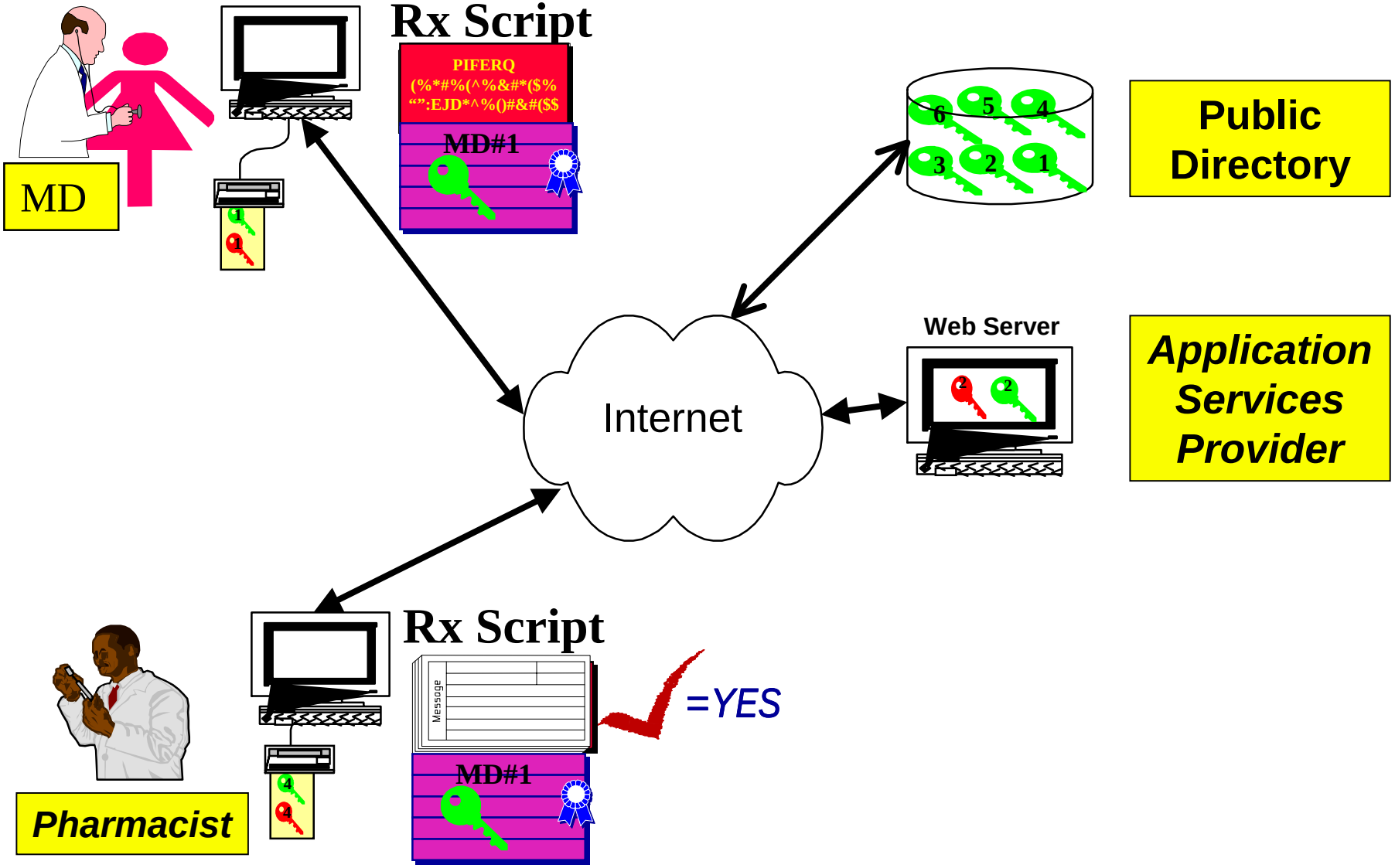
Pharmacist decrypts script



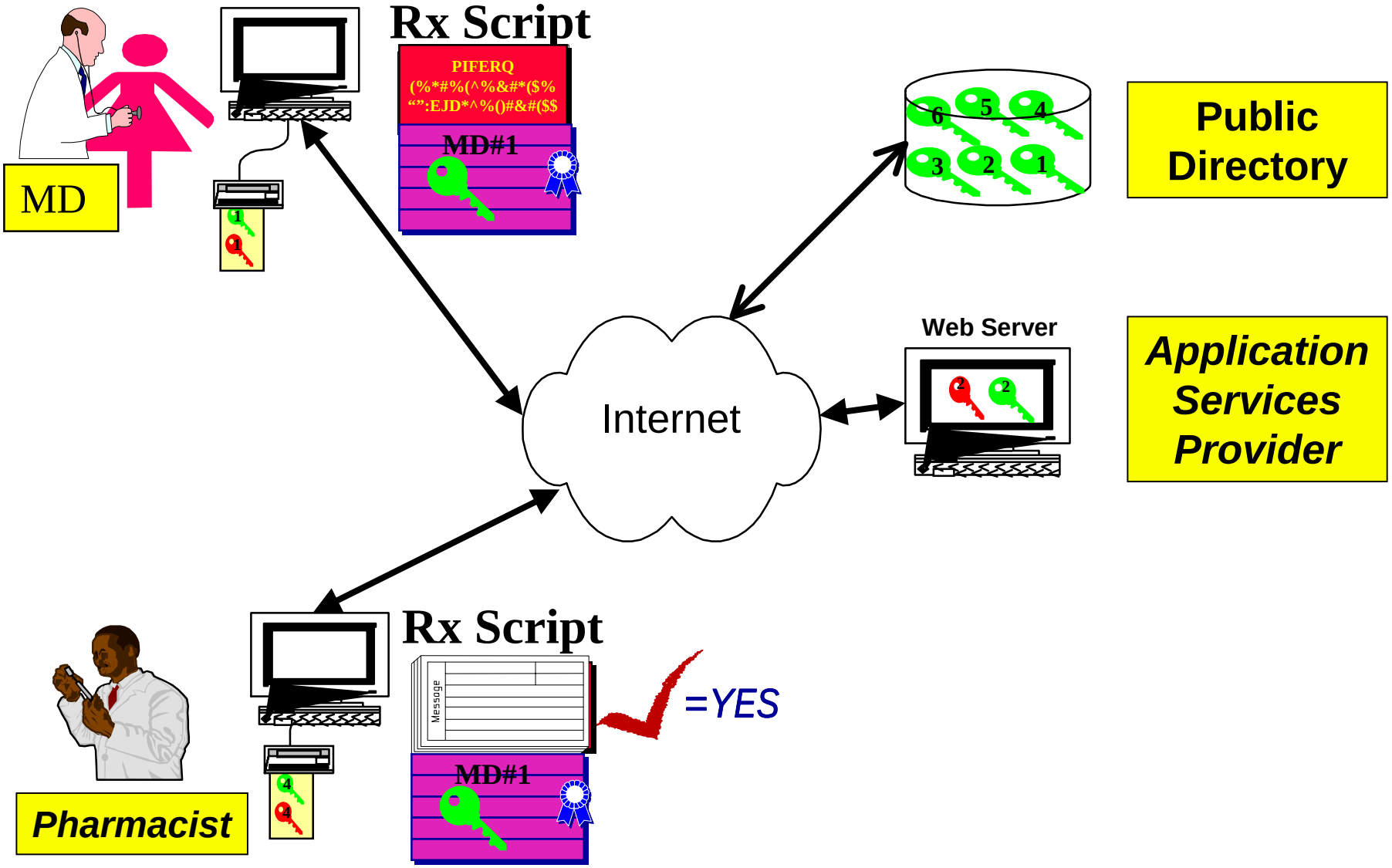
Pharmacist validates Script



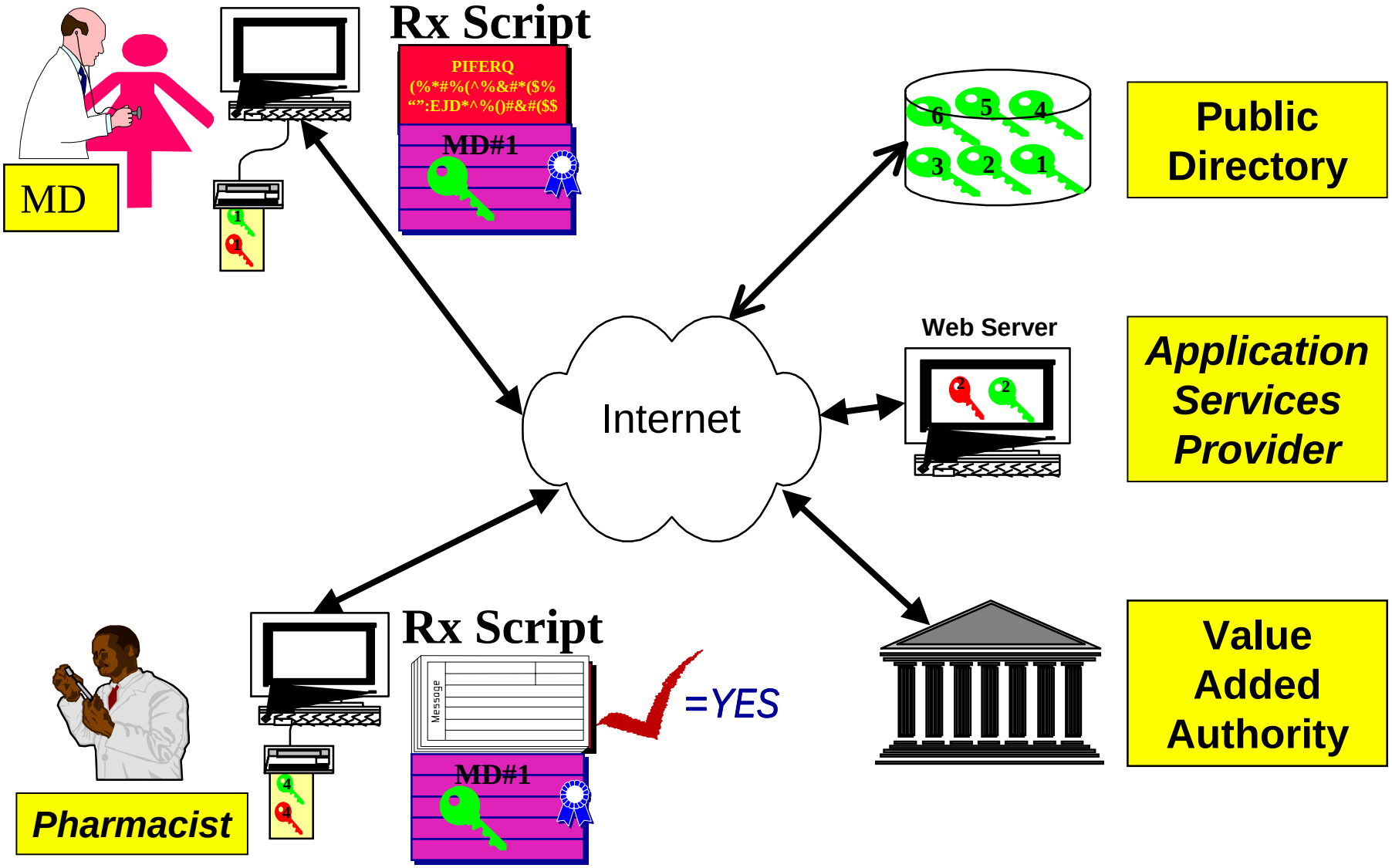
Pharmacist validates Script



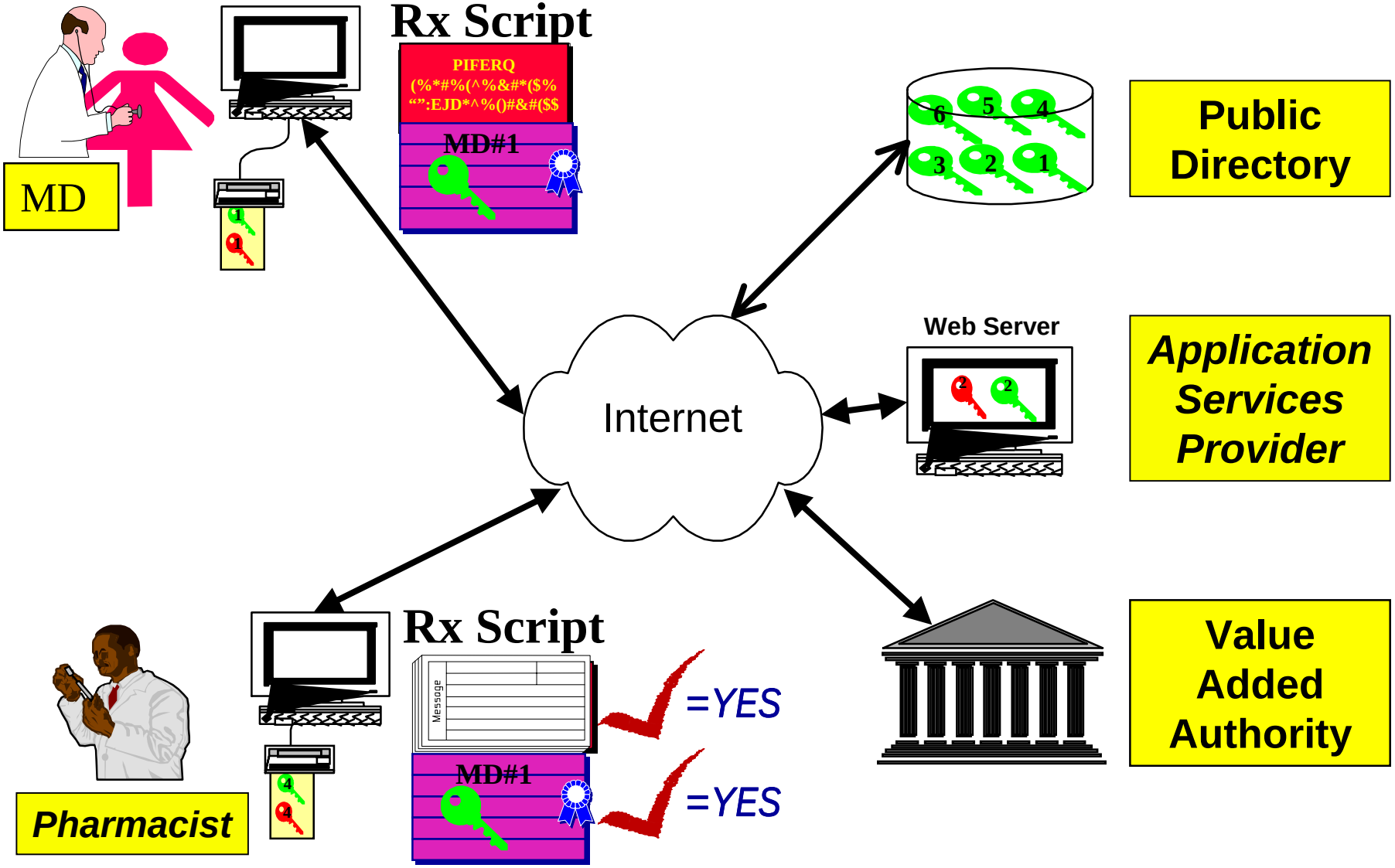
Pharmacy validates MD, Signatures



Pharmacy validates MD, Signatures



Pharmacy validates MD, Signatures



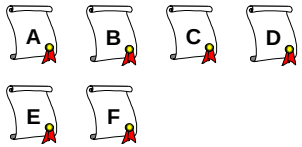
Healthcare Digital Signature Requirements:

- Chain-of-Trust/ interoperability Across the Healthcare Community established
- 24x7x365 reliability/availability (biometric sensitivity/central servers…)
- Standards based: X.509; LDAP; ASTM ????
- Trusted Healthcare root (CA) authenticating signature
- Professional healthcare credentials BOUND to identity.
- Non-repudiation thru user control of identity - no centralized, vulnerable storage; no backup.
- Signature validity tied to role based certificates: identity, multiple roles, credentials.
- Mobile Identity- sign anywhere
- One identity - Multiple uses: corporate badge; CPU; physical plant access.
- Distinguish signature certificate from encryption certificate.
- Differentiation of identities for patient, employer, licensed and board certified individuals.
- Certificate/signature validation in real time
- Transcend and incorporate state Jurisdictional variations ie. Licensure/signature.
- Integration of legacy systems.
- Non Reputable retention/validation for 25 years
- Multiple signatures
- Transcends industry boundaries (provider/Insurers/Employers/Patients)

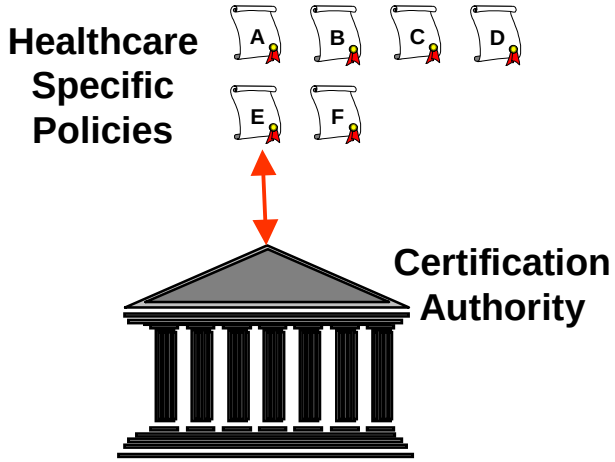
Enabling Solution:
Trusted Healthcare Identity Service

Enabling Solution:
Trusted Healthcare Identity Service

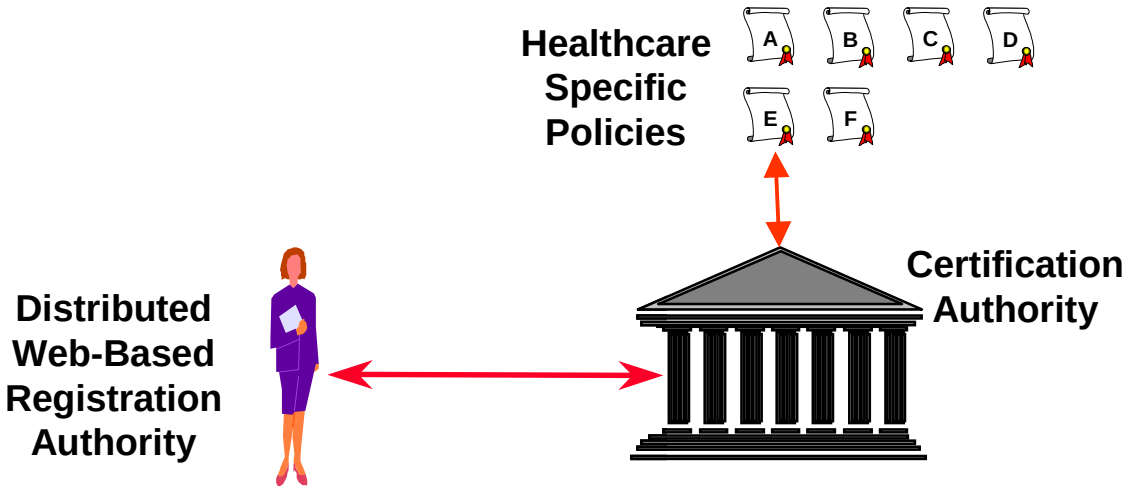
Healthcare Specific Policies



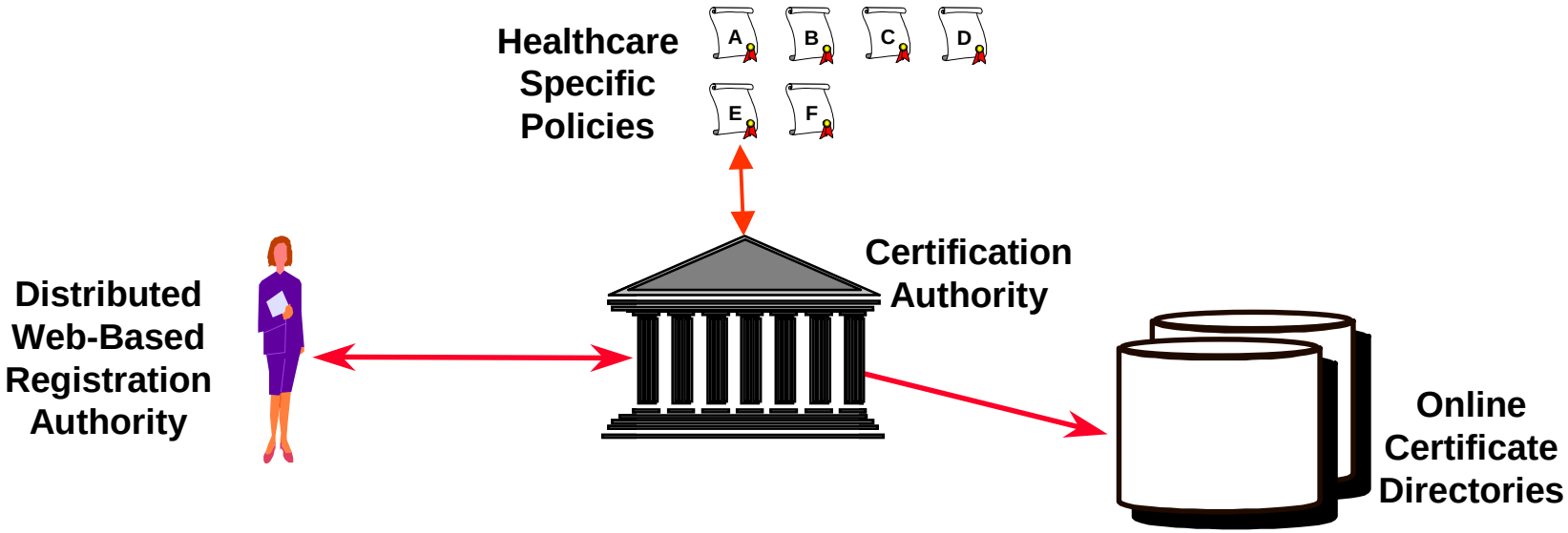
Enabling Solution:
Trusted Healthcare Identity Service



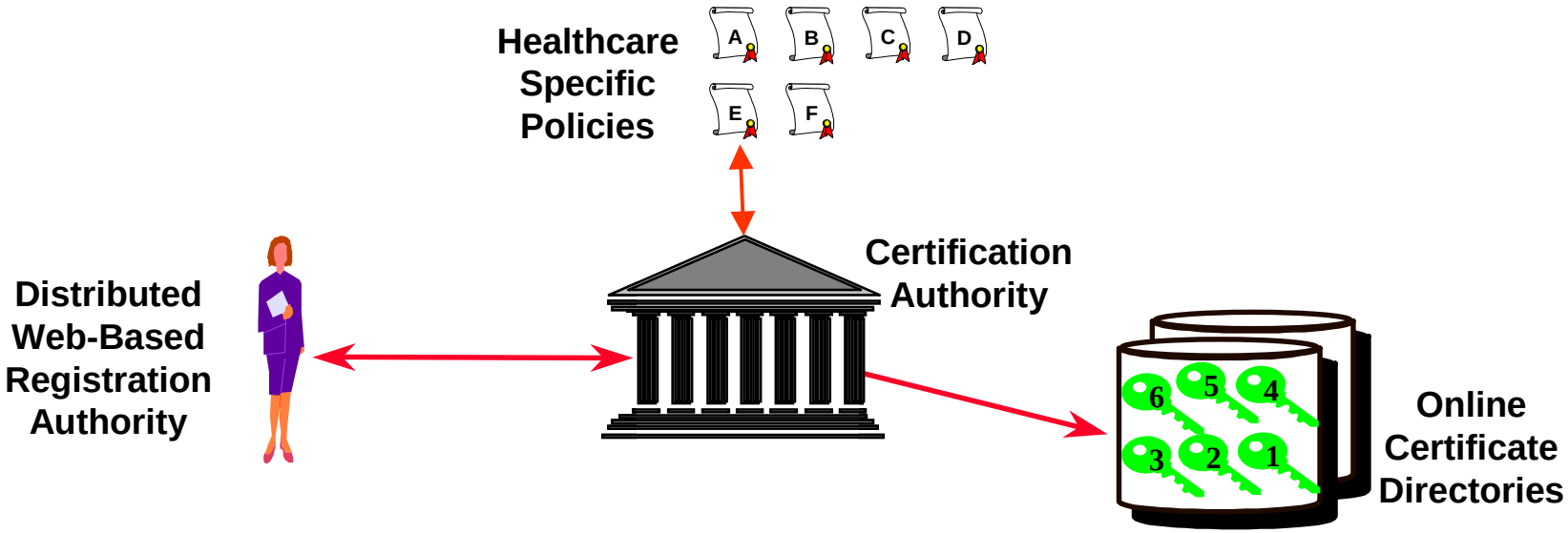
Enabling Solution:
Trusted Healthcare Identity Service



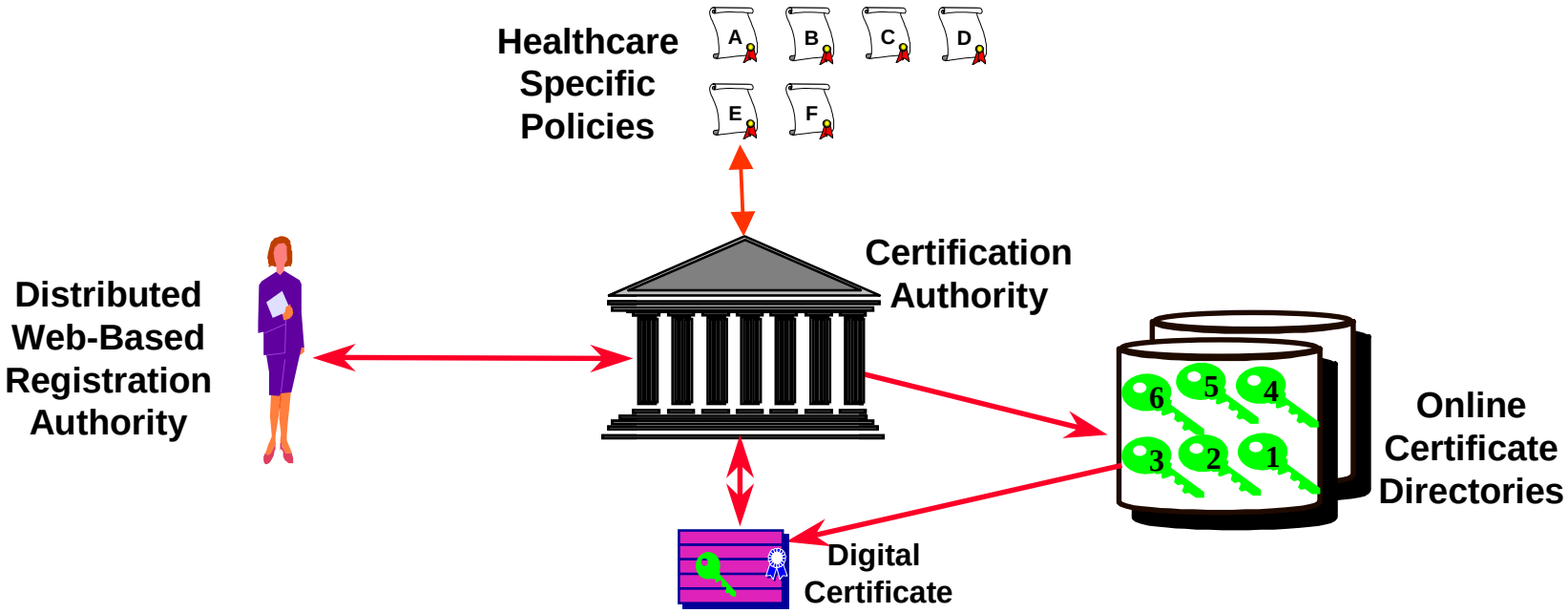
Enabling Solution:
Trusted Healthcare Identity Service



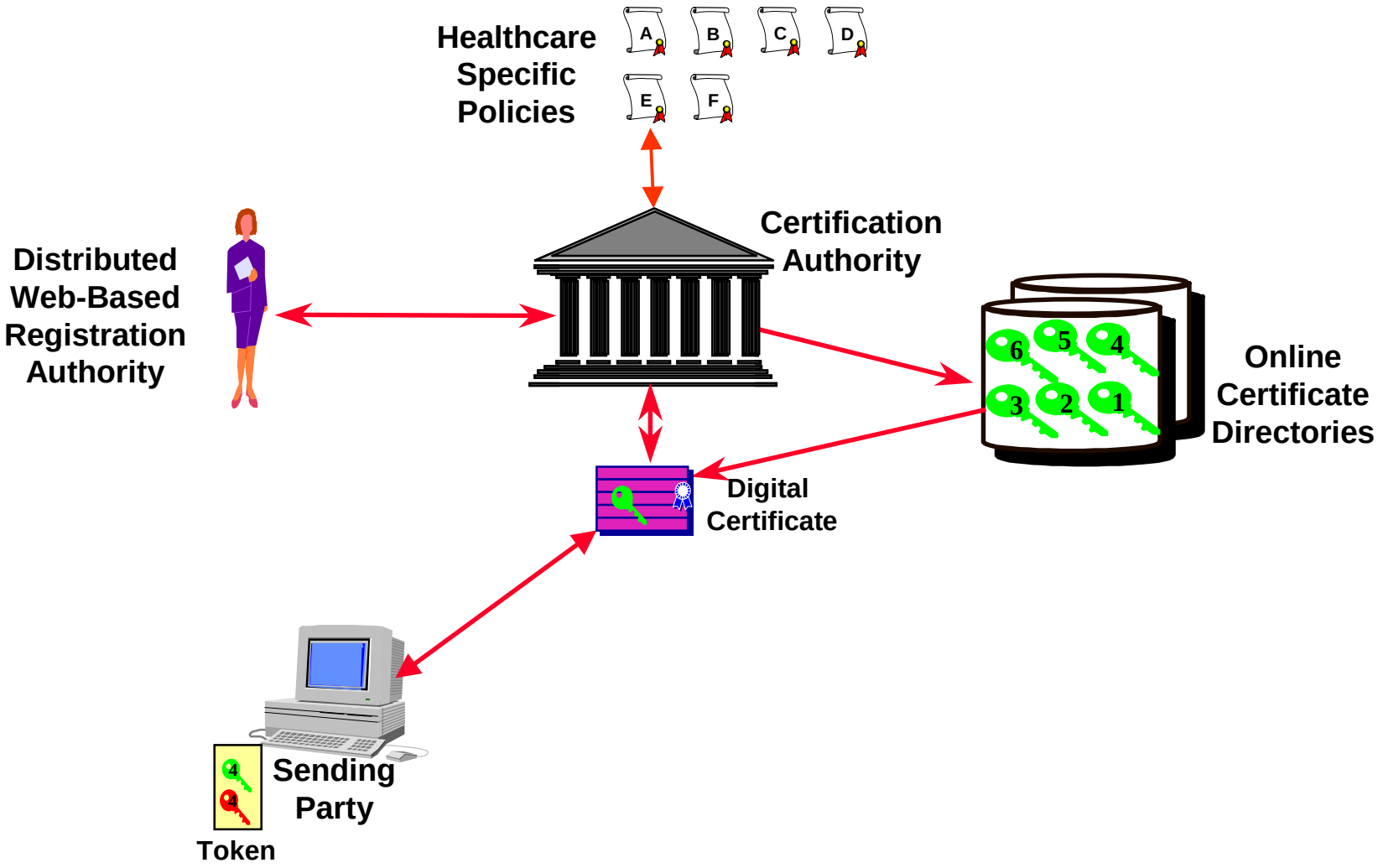
Enabling Solution:
Trusted Healthcare Identity Service



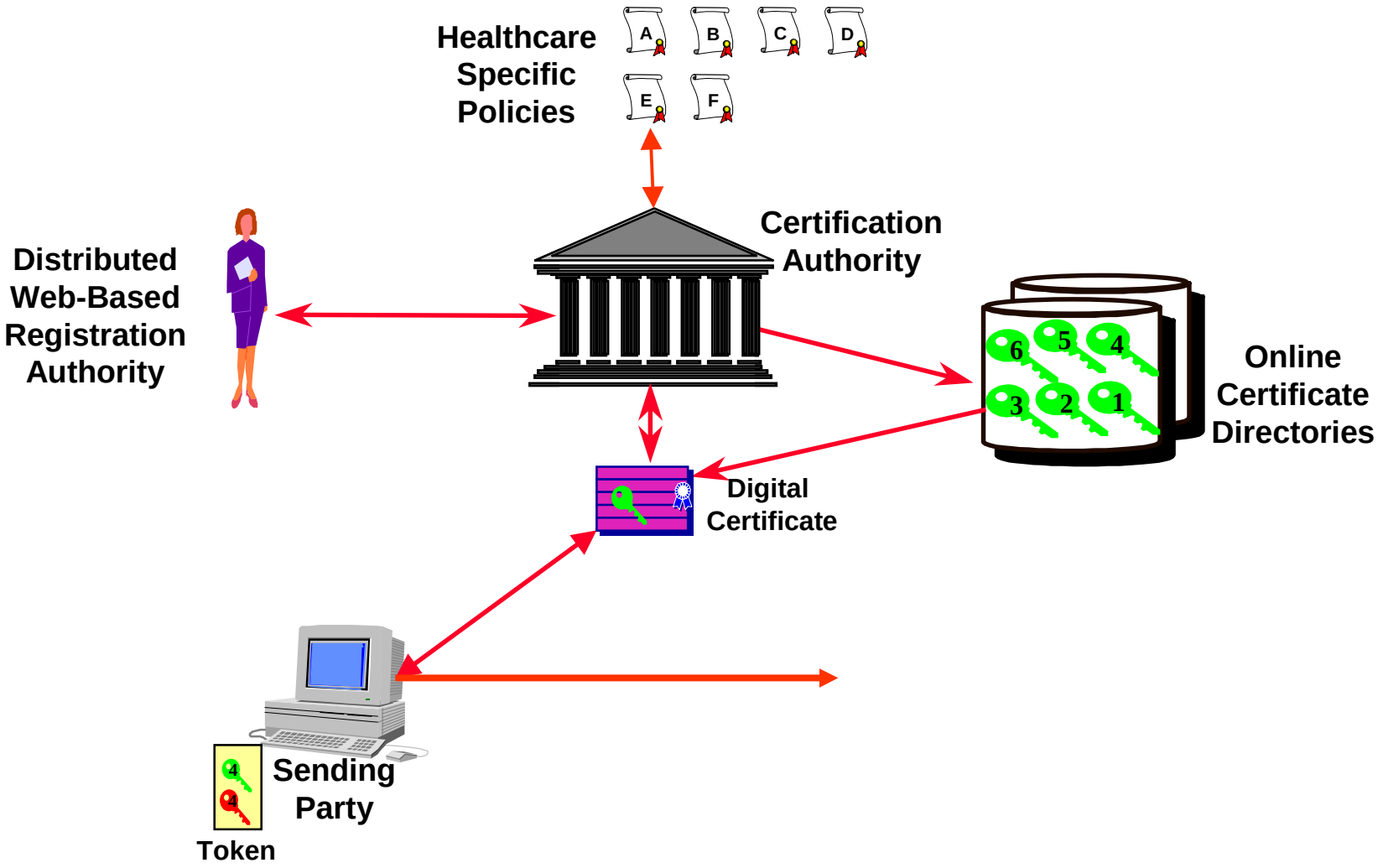
Enabling Solution:
Trusted Healthcare Identity Service



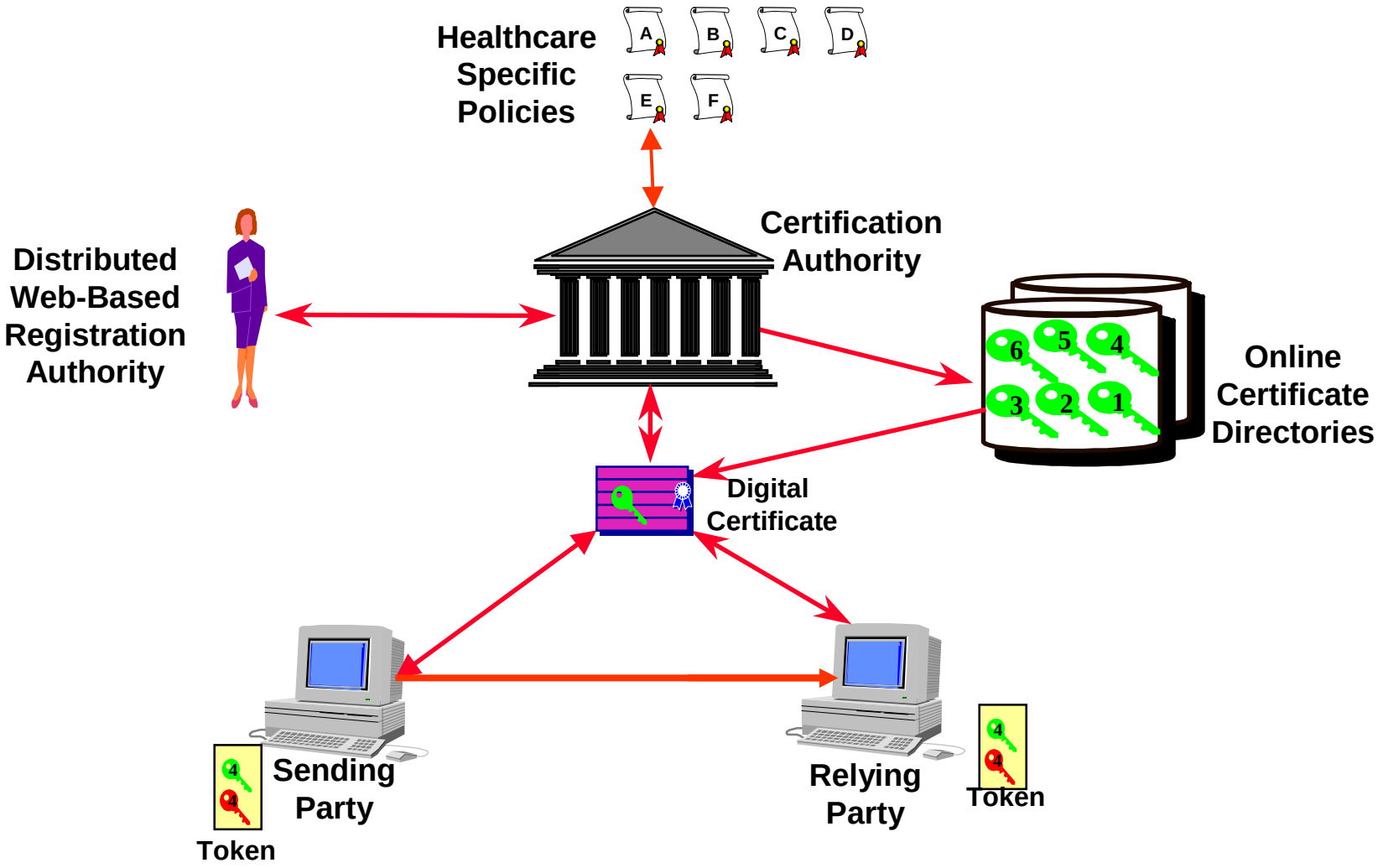
Enabling Solution:
Trusted Healthcare Identity Service



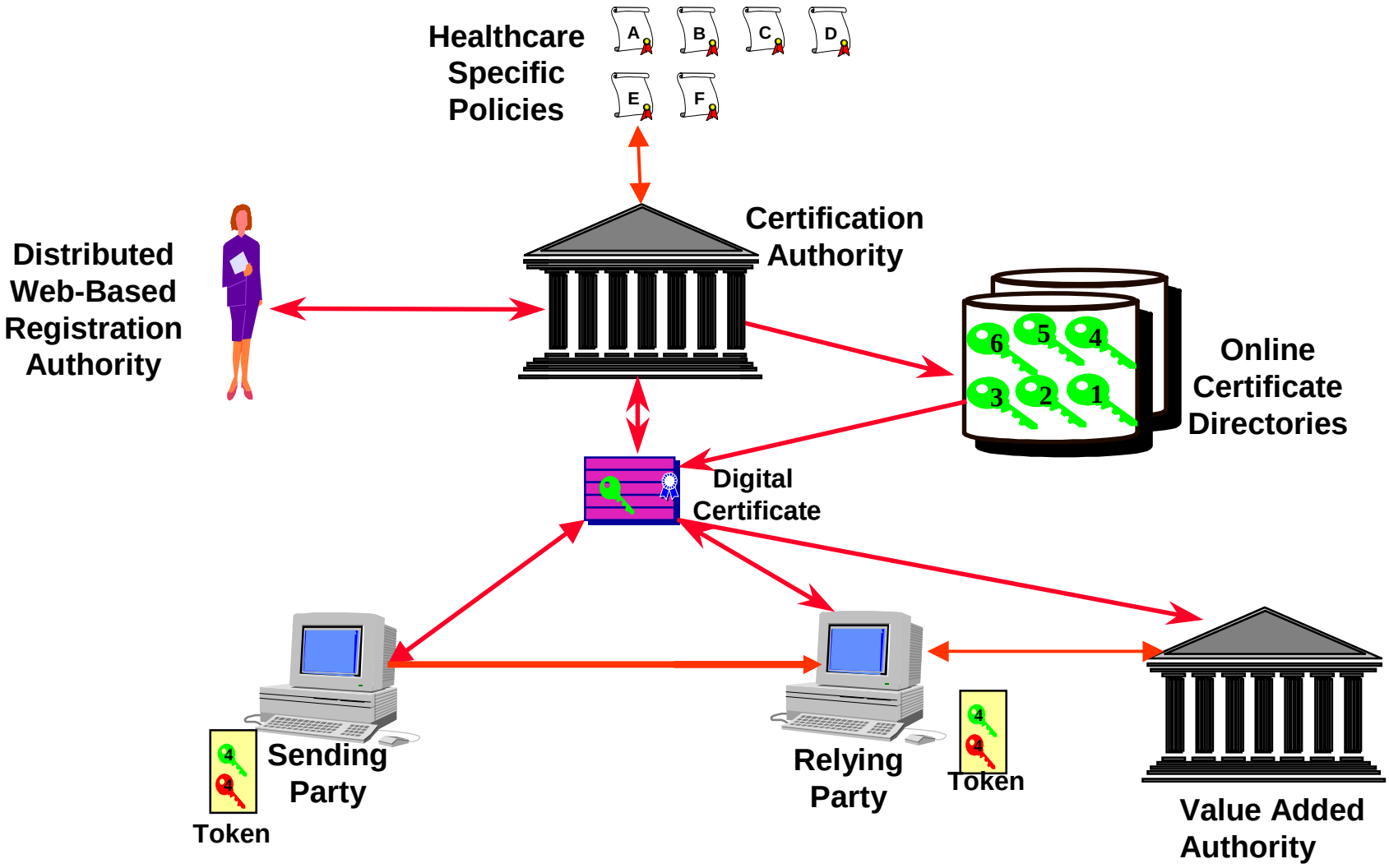
Enabling Solution: Trusted Healthcare Identity Service



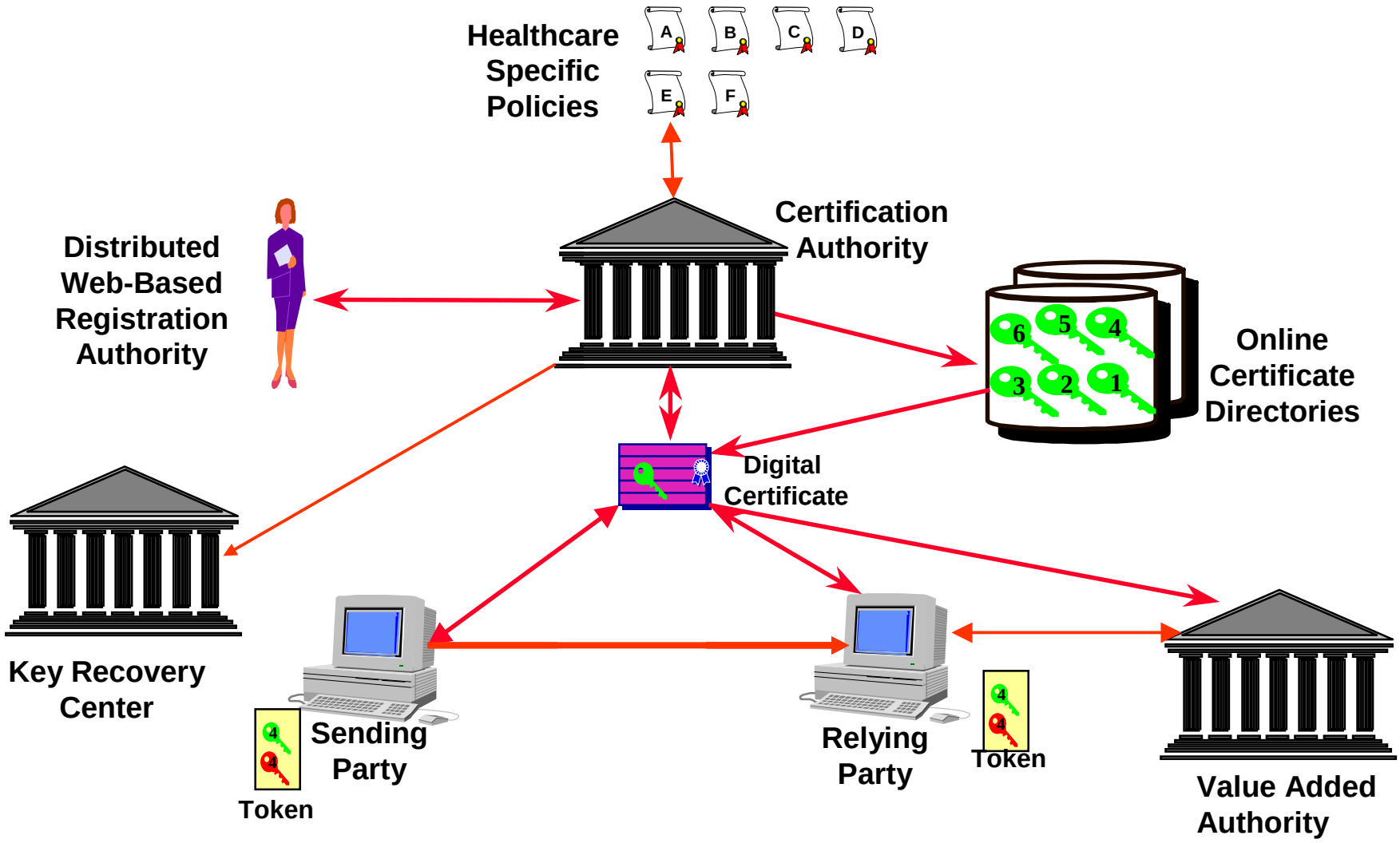
Enabling Solution:
Trusted Healthcare Identity Service



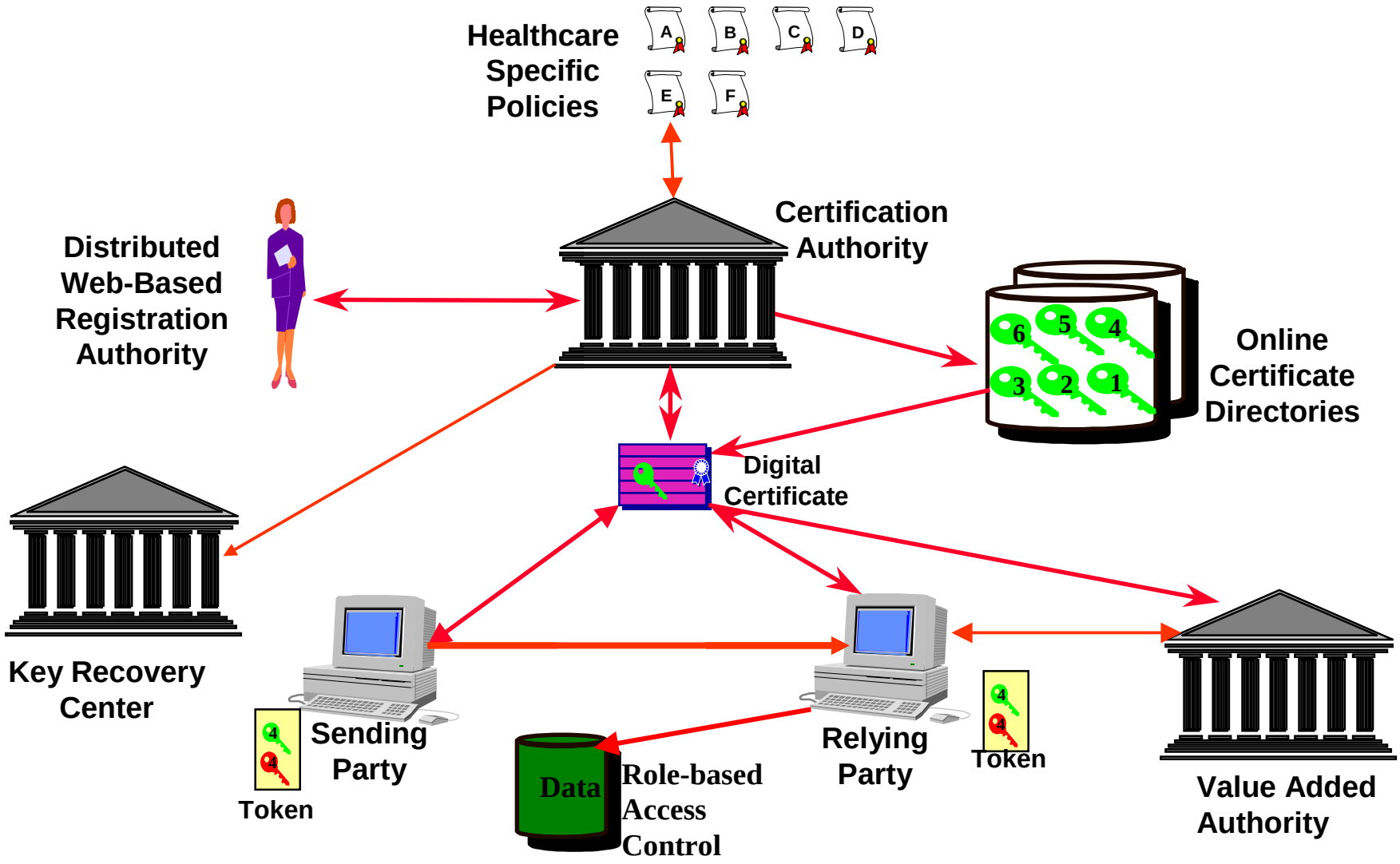
Enabling Solution:
Trusted Healthcare Identity Service



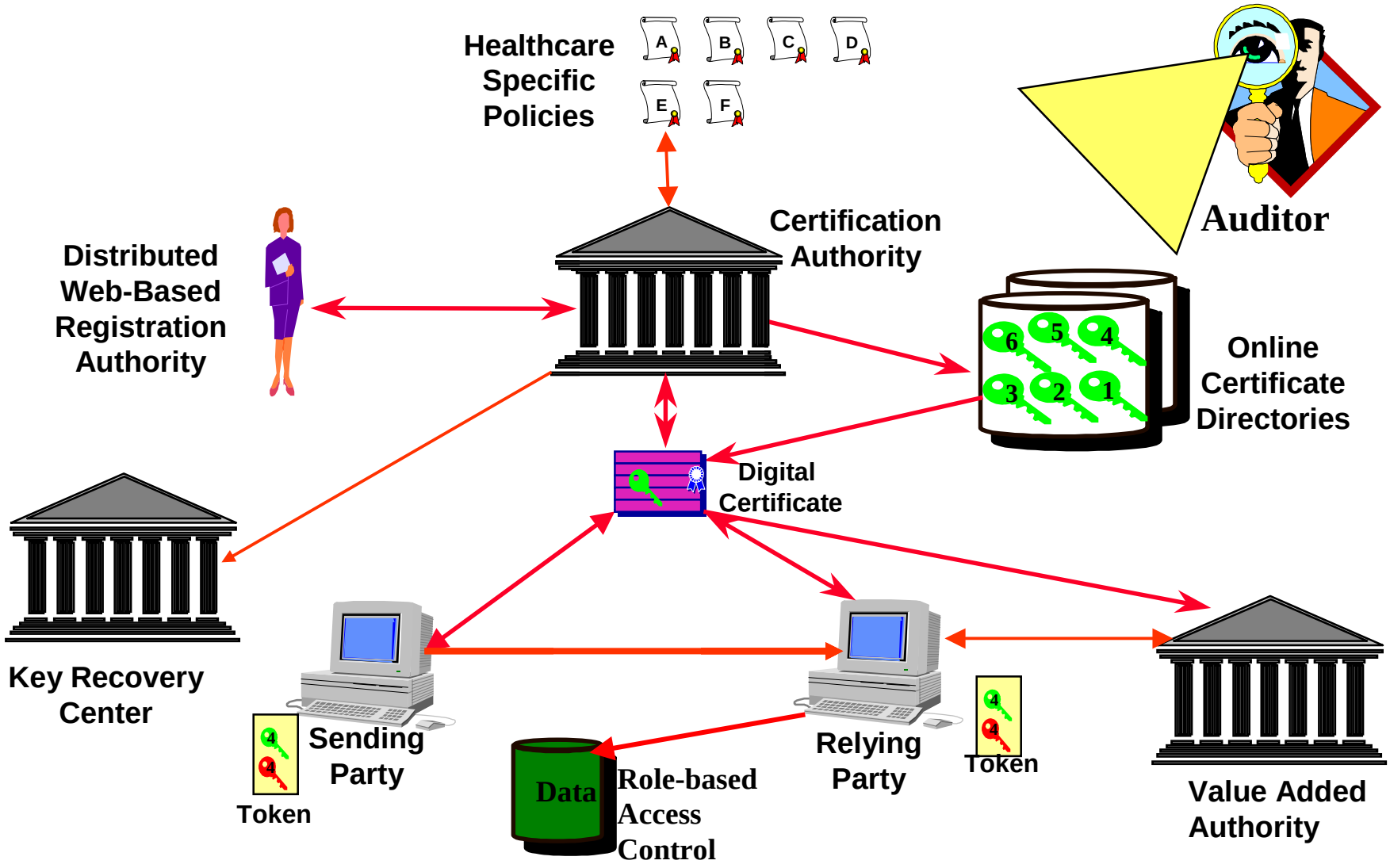
Enabling Solution: Trusted Healthcare Identity Service



Enabling Solution:
Trusted Healthcare Identity Service



Enabling Solution:
Trusted Healthcare Identity Service

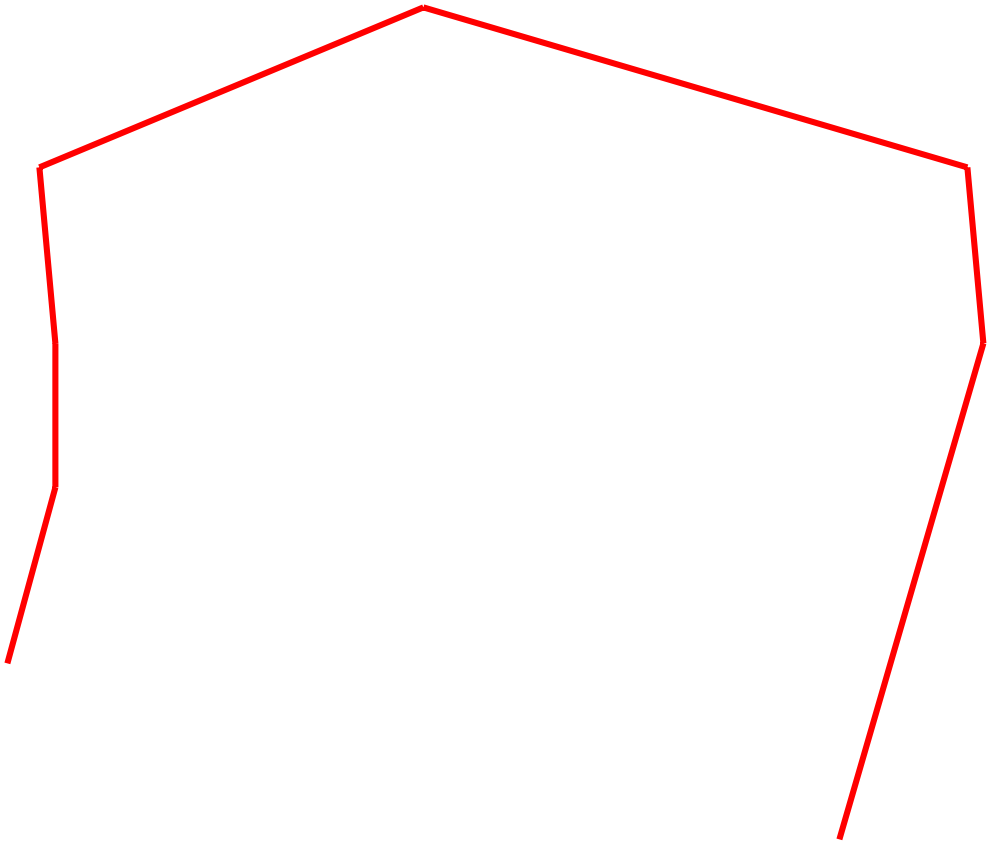


Healthcare Policy **Types**

- Patient
- Employee
- Licensed Health Care Professional
- Board Certified Professional

- Organizational(Payer/Employer/etc.)
- Licensed Healthcare Organization (Hospital/Pharmacy/etc)

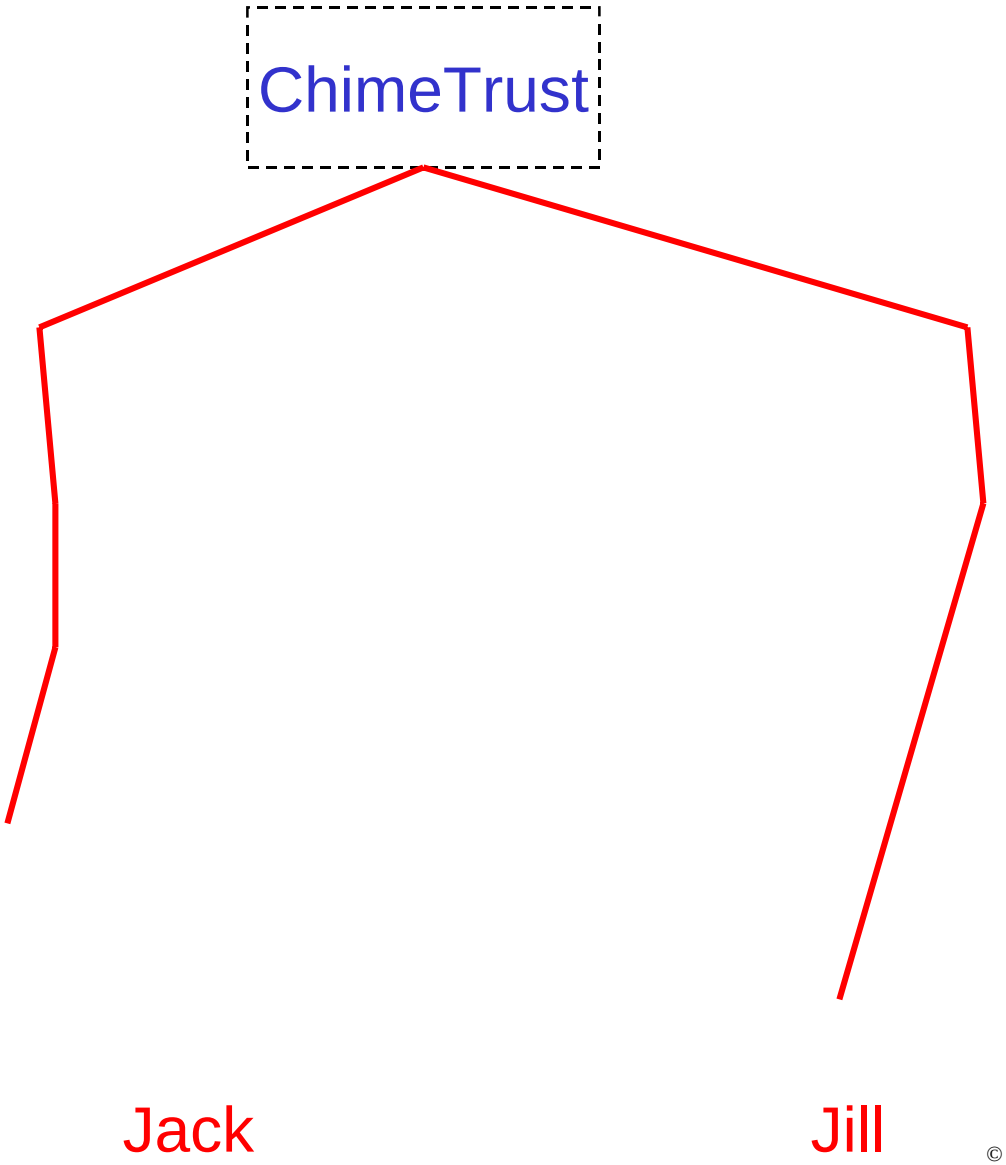
ChimeTrust
Chain of Trust



Jack

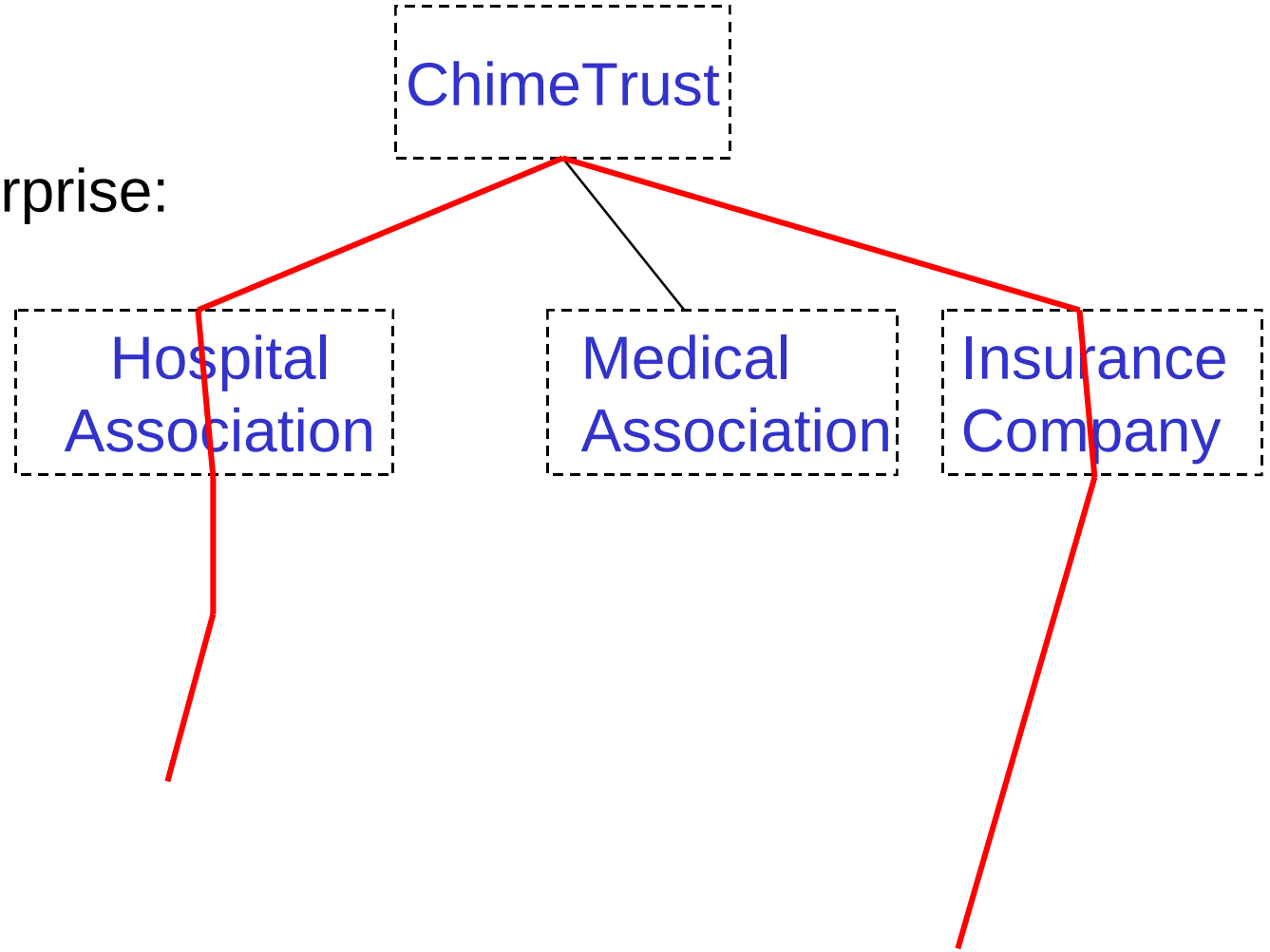
Jill

ChimeTrust
Chain of Trust

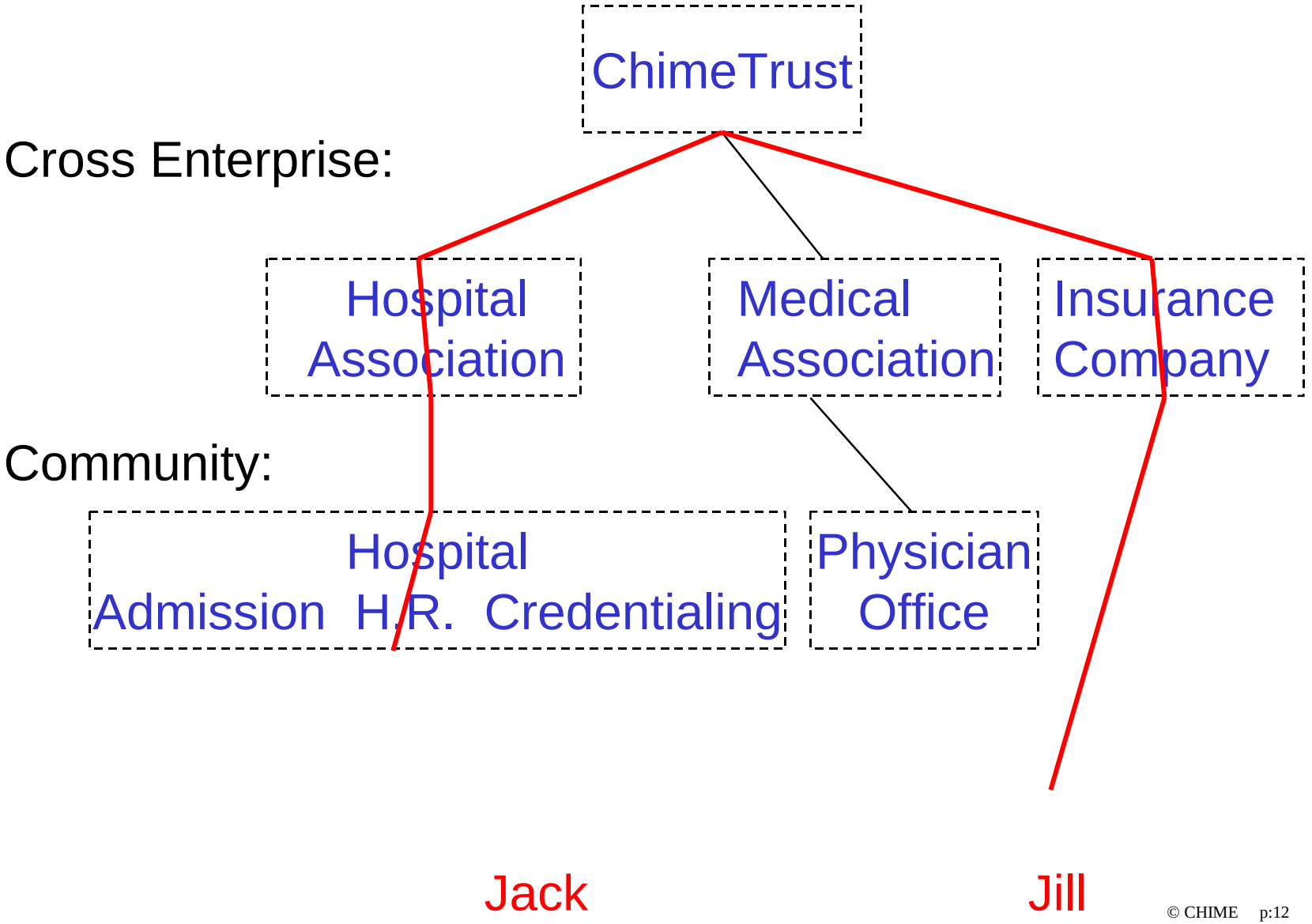


ChimeTrust
Chain of Trust

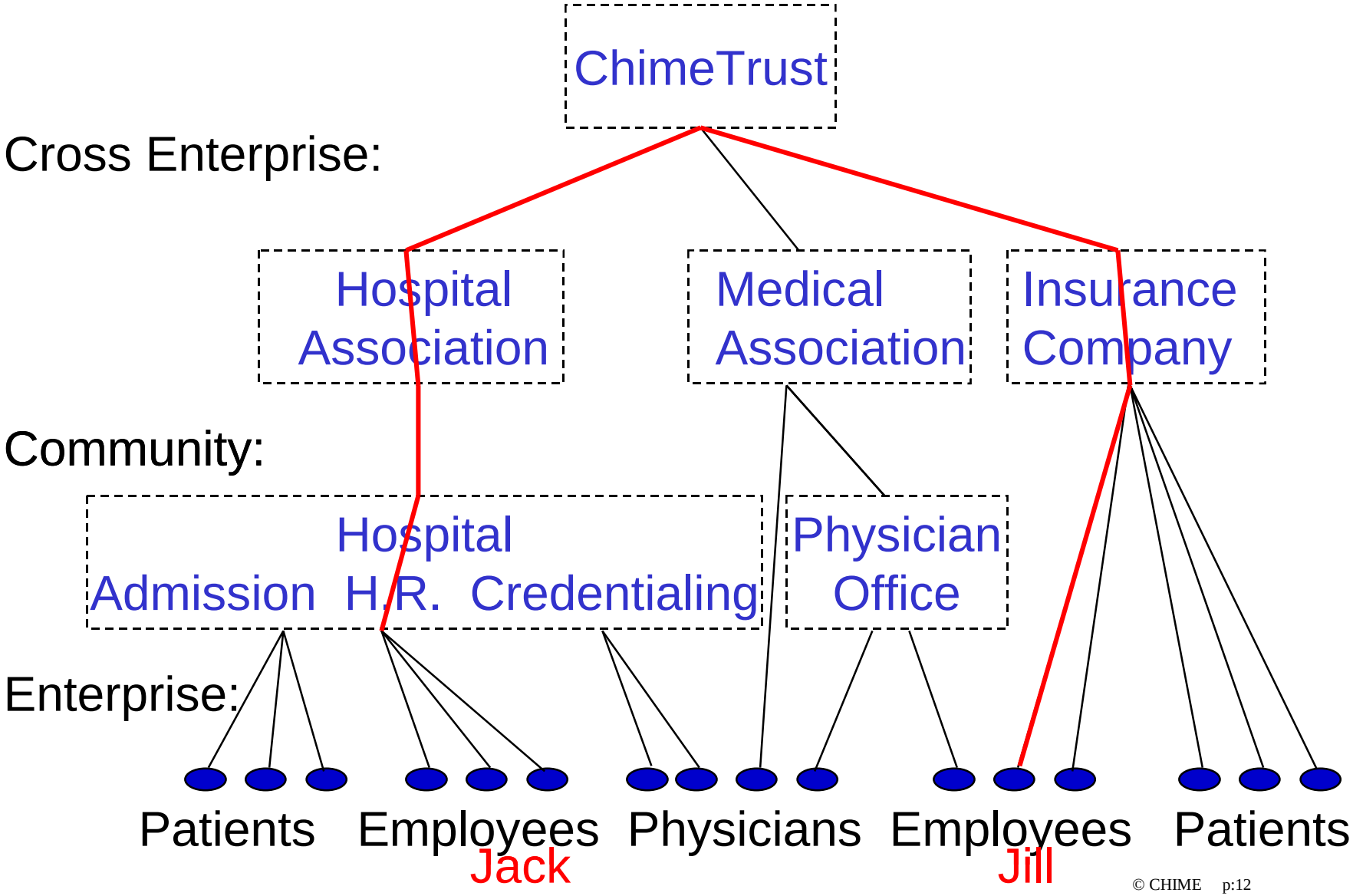
Cross Enterprise:



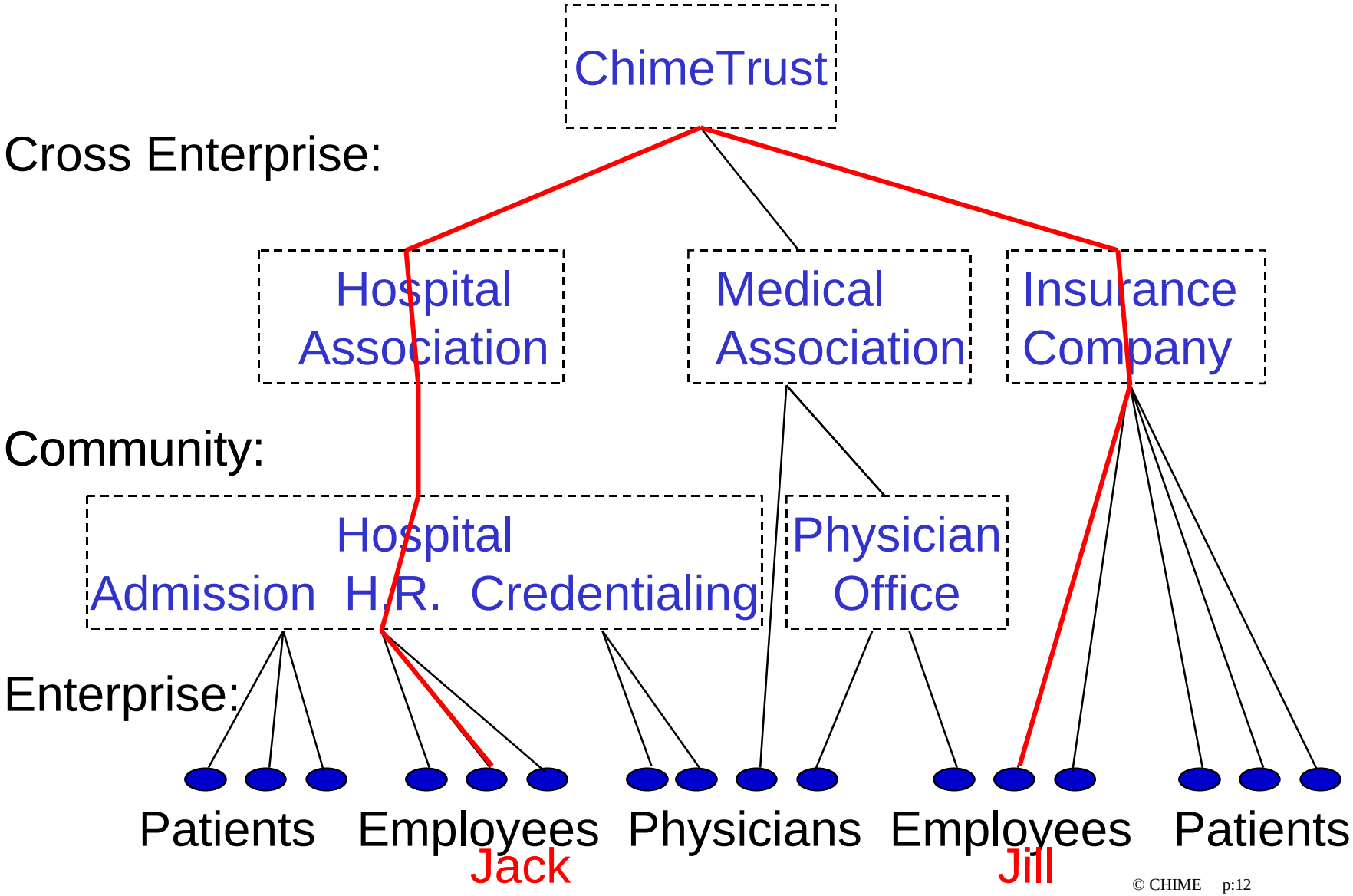
ChimeTrust
Chain of Trust



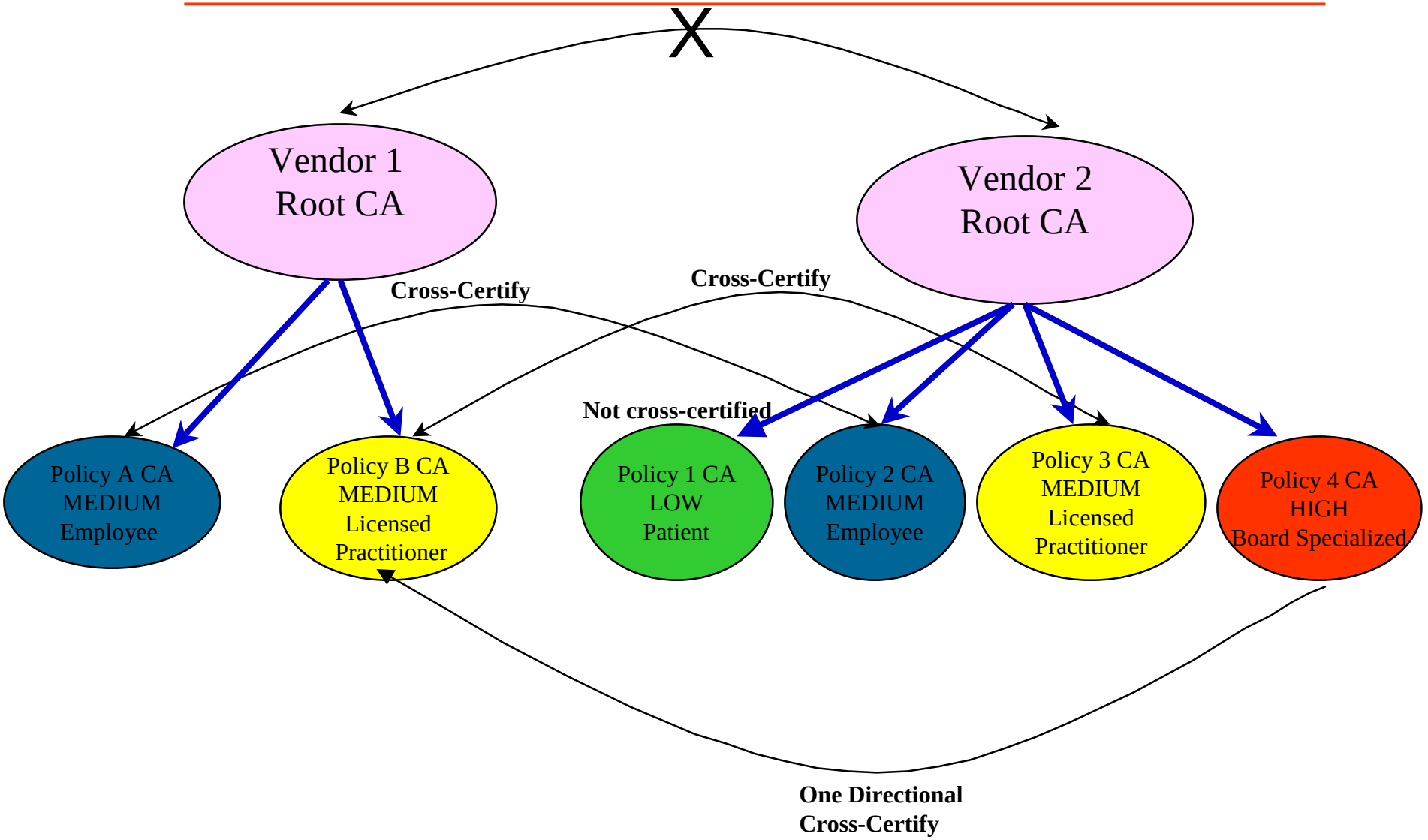
ChimeTrust
Chain of Trust



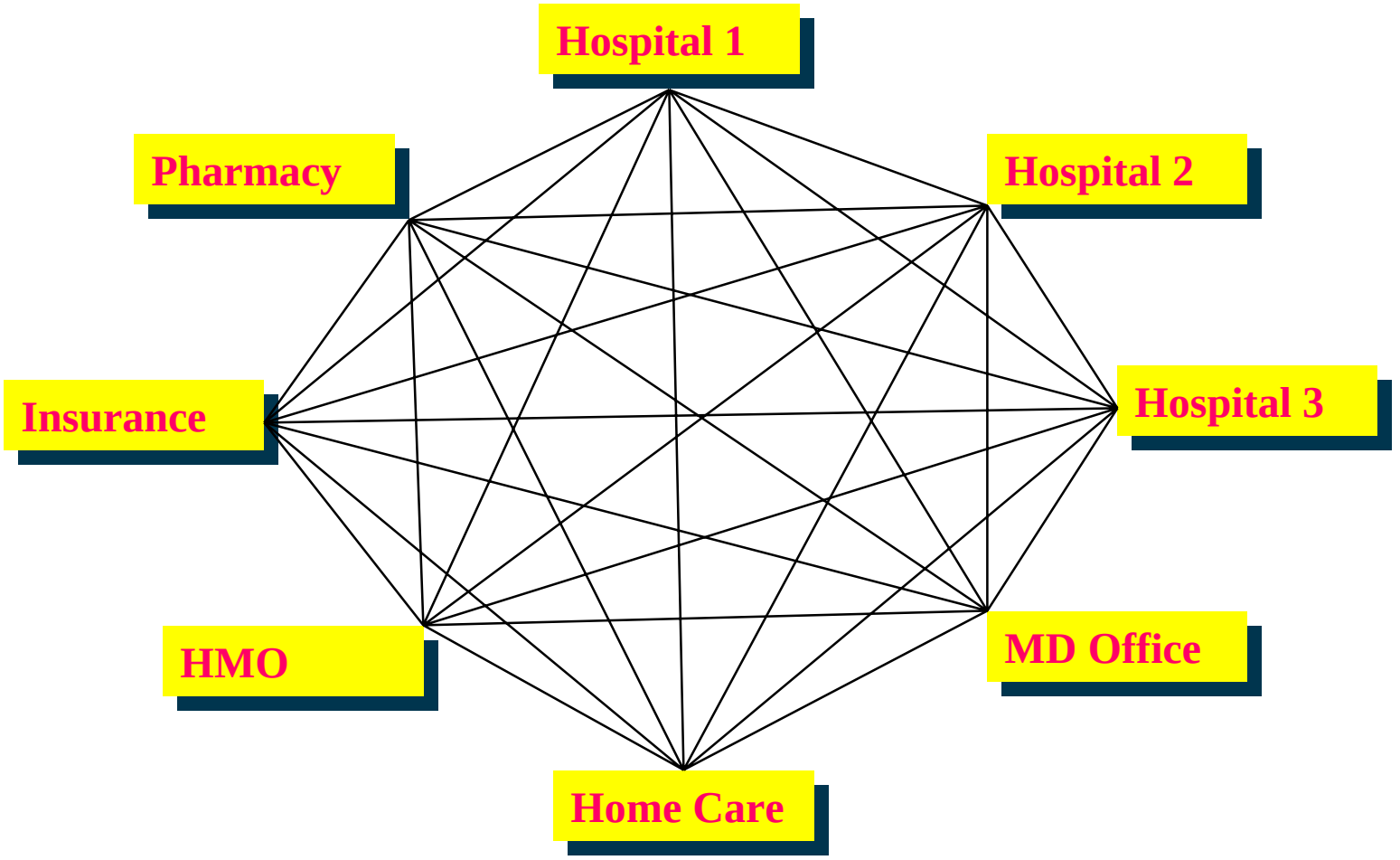
ChimeTrust
Chain of Trust



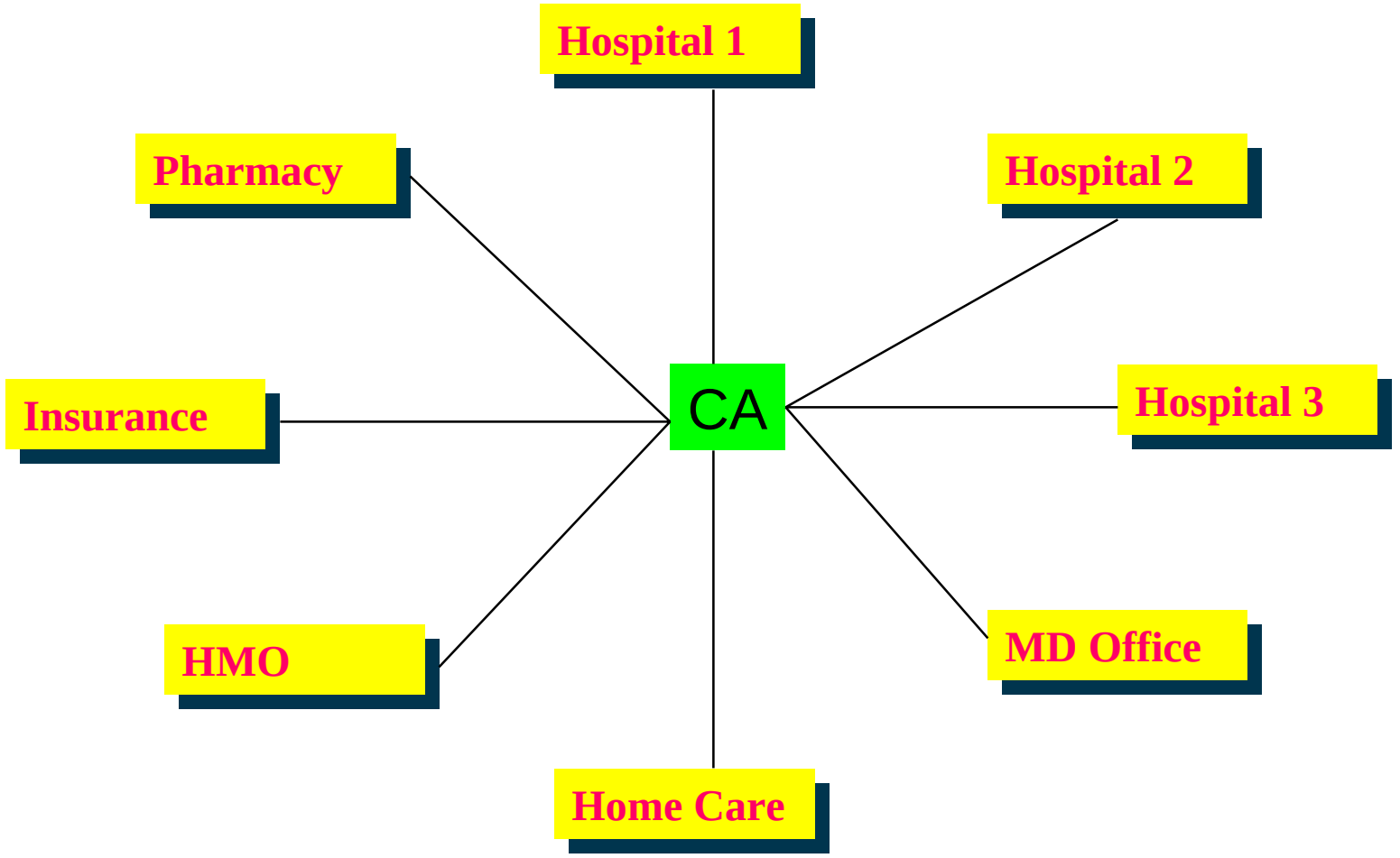
Policy Cross-Certification Issues



Trading Partner Agreements



Trading Partner Agreements
New Business Case



Federal PKI Semantic Framework (4)

- Backup of Signature Keys
  - Rudimentary: Not backed up
  - Basic: Must not be backed up
  - Medium: Must not be backed up
  - High: Must not be backed up

Source: PKI Certificate Policy Requirements Analysis; Revised Draft, February 18, 2000; PEC Solutions, Inc.

Federal PKI Semantic Framework (10)

- CA standard for proof of identity from certificate applicant
  - Rudimentary: No Proof required: on-line or in person with 2 IDs
  - Basic: Proof required: on-line or in person with 2 IDs
  - Medium: Proof required: on-line or in person with 2 Ids incl. 1 government picture ID
  - High: Proof required: in person required with 2 IDs incl 1 government picture ID

Source: PKI Certificate Policy Requirements Analysis; Revised Draft, February 18, 2000; PEC Solutions, Inc.

Verification Requirements: Individual

- A **government issued photographic Identification**
- A **second form of identification**: social security card, Credit card, utility bill, birth certificate, tax form
- **Subscriber ID** for Insurance Plan or Health Care System
- **Employee ID** or letter from employer on employer letterhead indicating current employment status.
- Certificate **Request/Contract** duly signed.
- Certified, State-Issued Healthcare **License**
- **DEA** Number
- Certified **Board-certification** Certificate

Federal PKI Semantic Framework (11)

- Requirements of CA record maintenance
  - Rudimentary: No requirement
  - Basic: At least 7.5 years
  - Medium: At least 10.5 years
  - High: At least 20.5 years

Source: PKI Certificate Policy Requirements Analysis; Revised Draft, February 18, 2000; PEC Solutions, Inc.

Federal PKI Semantic Framework (14)

- End entity Private key protection requirement
  - Rudimentary: No requirement
  - Basic: May be in hardware or software
  - Medium: May be in hardware or software
  - High: Must be in hardware

Source: PKI Certificate Policy Requirements Analysis; Revised Draft, February 18, 2000; PEC Solutions, Inc.

Digital Certificates On Smart Cards

Front

DOE

John Doe, M.D.

Pediatrics

Employer's Logo

Back

If Found, Return to:

CHIME-Trust
P.O. Box 90
110 Barnes Road
Wallingford, Ct. 06492

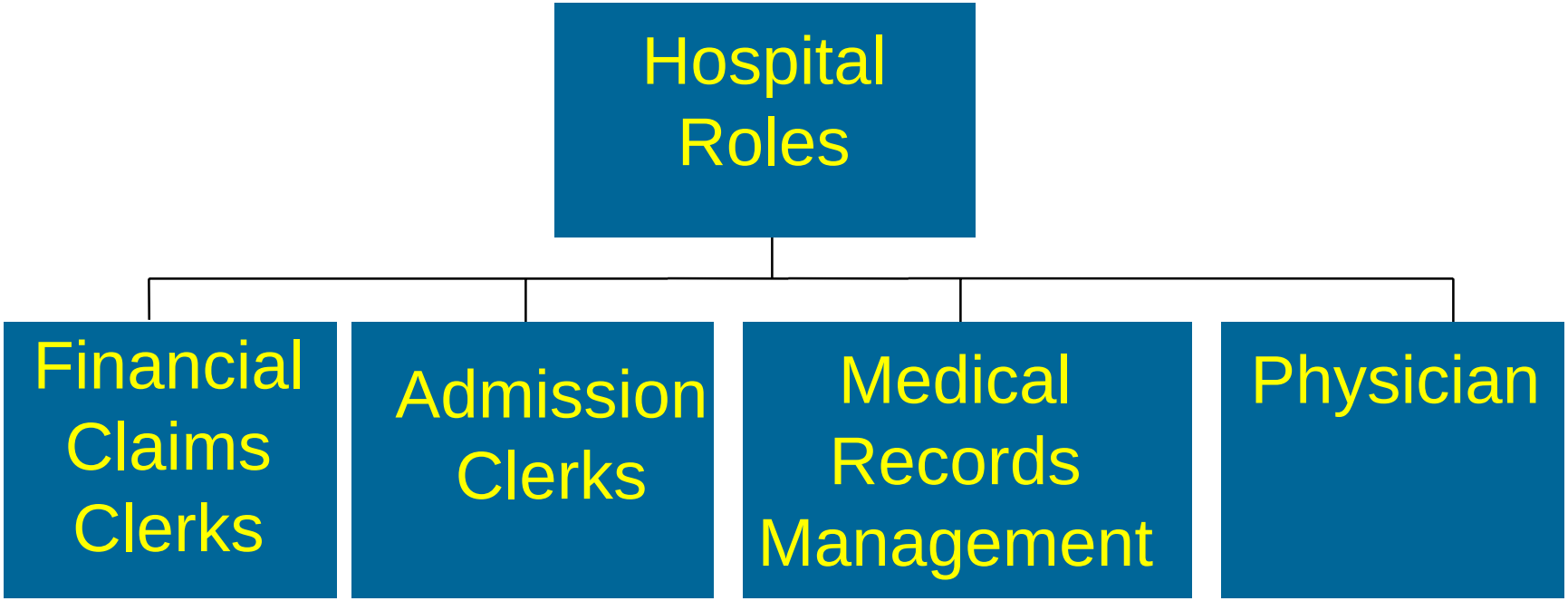
Help-Line:
(203) 294-7394
registrar@chime.net

Federal PKI Semantic Framework (16)

- Extent of damage if end entity signing private key compromised
  - Rudimentary: No injury or loss
  - Basic: Minor injury
  - Medium: Potential significant financial loss or require legal action for correction
  - High: Potential loss of life, imprisonment, or major financial loss

Source: PKI Certificate Policy Requirements Analysis; Revised Draft, February 18, 2000; PEC Solutions, Inc.

Example: Organizational Authority



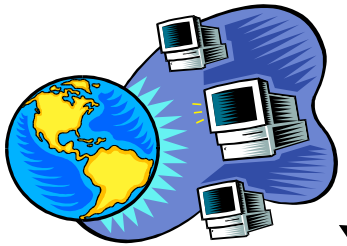
Based upon ASTM Standards

Secured Applications

Prescription Fulfillment

Patient Record Review

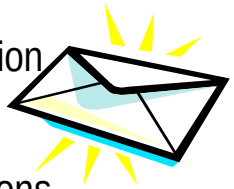
Research Collaboration



Consultation

Referrals

Prescriptions



E-mail

Patient Record/History Review

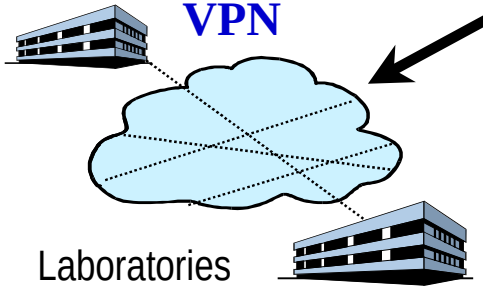
Verification of Insurance Eligibility

Secure Desktop

Web

PKI

VPN



Laboratories

Multi-Hospital/Clinic

Report Review/Approval

Caregiver Access to Patient Record/History

Generate orders

****

Single Login

E-Commerce

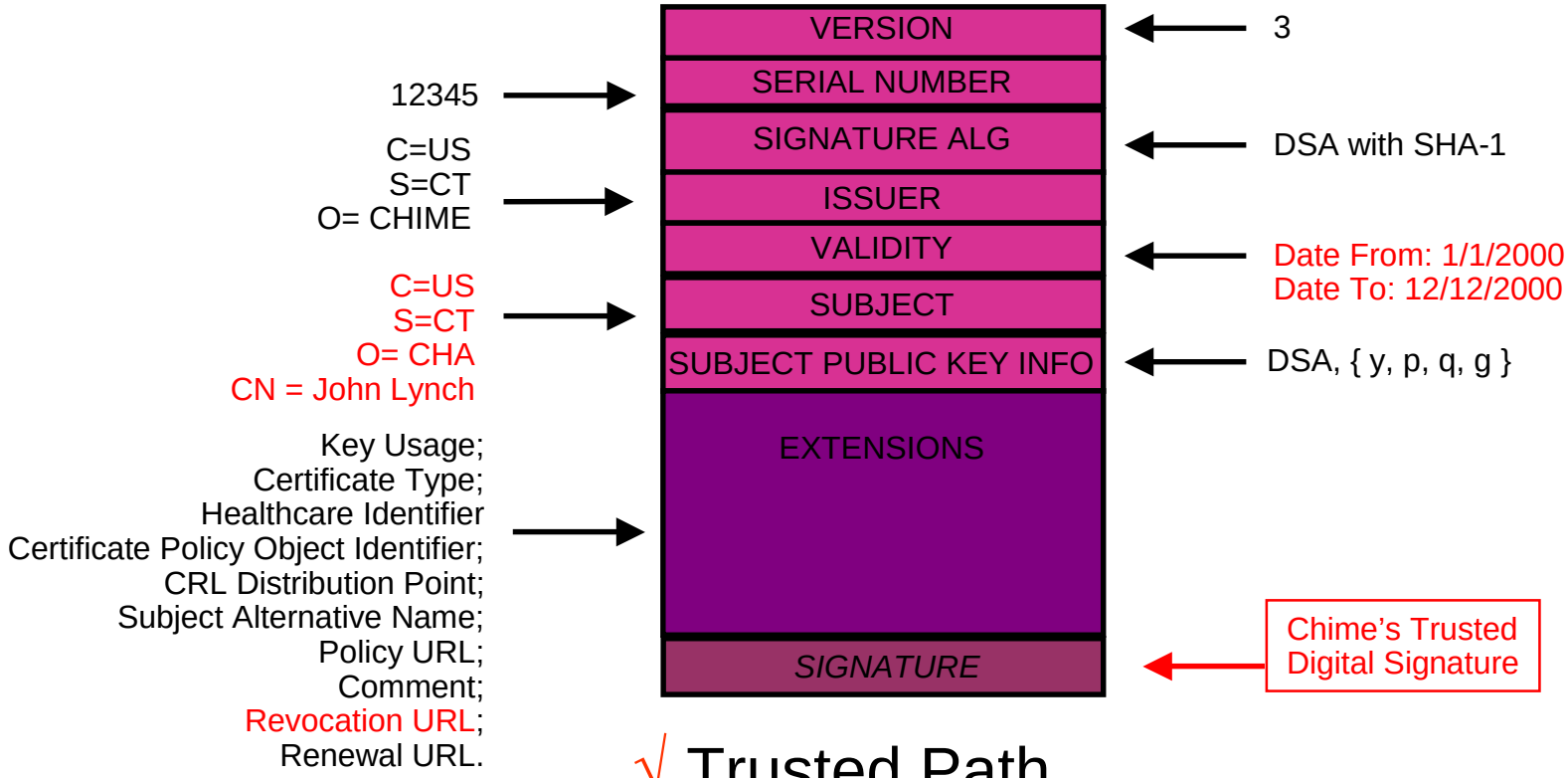
EDI/Claims Processing/Payment

Accounting and Billing

Payment to Vendors/Suppliers

Demo e-mail Signatures

Requirement:
Digital Signature Validation



- √ Trusted Path
- √ Trusted Signature
- √ Valid Dates
- √ Not Revoked

Healthcare Applications

- Lanier - Dictation/transcription
- Blue Cross: Web access/eligibility
- Hospitals: web retrieval lab/results
- physical access
- Orders
  - Prescriptions
- Observations/Findings
- Documents requiring signatures (gov forms)
  - W10 referrals

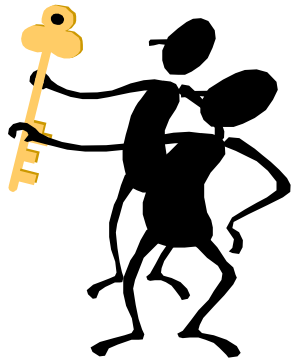
Issues

- Cannot look at digital signature in isolation
- Microsoft Outlook example:
  - e-mail on cert must = sendor e-mail
  - forwarded e-mail drops signature
  - Cannot discriminate encryption/signature cert
  - e-mail “from” field not necessarily sendor
  - accepts preloaded generic trust
  - No way to automatically define OID trust
  - No multiple signatures
- Details in cert - no validity test by COTS
- Biometrics NOT signature, no standards

Recommendations:

- Standard Policies/DEA/Federal (VA…)/employee…enabling not mandated…common OIDS…create TRUST
- Bridge at policy level - HHS say equal…Crate TRUST
- Standard Credentials/Authority within healthcare
- Standard audit/License of CA/RA to meet Medicare policy-evaluate using Federal Semantic framework and policies…Create TRUST
- Education of providers/payers
- Cross state standards
- Lead by example - HHS use PKI, require for Medicare data
- Allow CA intermediary in trading partner agreements
- Allow CA to be Provider Identifier issuer
- Create testbeds ie NJ for DRGs
- Work vendors ie Microsoft,... with requirements

Together - We Hold the Key !



Health PKI

For more information contact:

John Lynch
President and CEO
HealthPKI
7 Buttonwood Circle
Cheshire, Ct. 06410-4305
phone: (203)272-0132
e-mail: jtlynch@snet.net